Draft Study Material

JOB ROLE

CYBER SECURITY ASSISTANT

Qualification Pack
QG-03-IT-00350-2023-V1-NIELIT

Sector: IT-ITeS
Grades: X

विद्यया ऽमृतमश्नुते

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

Cyber Security Assistant

Grade – X

Qualification Pack
QG-03-IT-00350-2023-V1-NIELIT

PSS Central Institute of Vocational Education

(A constituent unit of NCERT, under the 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.

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,

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

PREFACE

The National Education Policy, 2020, emphasizes removing hard distinctions 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 that 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

Foreword

Vocational Education and Training (VET) plays a significant role in preparing youth for relevant occupations and meeting the skill demand of the changing labour market. This is even more relevant, as India is witnessing an accelerated youth population and the need for preparing a skilled workforce for the growing economy. The strong partnership with the industry partners characterises India's National Skills 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 the National Educational Policy (NEP) 2020 have focused on making the 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, to develop a pool of trained vocational teachers or resource persons in spearheading the effective, Implementation of the scheme an vocationalization 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 to provide 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 Assistant for Class 10th" is a structured and application-oriented textbook designed to strengthen students' understanding of cyber security concepts and modern digital threats. It builds on foundational knowledge and focuses on protecting systems, networks, and applications in real-world computing environments.

The textbook covers essential topics such as Cyber Security fundamentals, Ethical Hacking and Cryptography, Operating System Security, Security Tools for Windows OS, Wireless Networks and Security, Mobile OS Security (Android and iOS), and Web Application Protocols and Browser Security. Each chapter presents concepts in a clear and student-friendly manner, supported by examples and practical activities to develop analytical and defensive skills.

Through this book, students learn how cyber attacks occur, how security mechanisms work, and how to apply protective measures across different platforms. The textbook promotes responsible digital behavior, critical thinking, and hands-on learning, preparing students for advanced studies and future careers in cyber security and information technology.

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, GNCT, Delhi
4. Ms. Yogita Goyal, Gurukul The School, Ghaziabad
5. Dr. Monika Sharma, PSSCIVE, Bhopal
6. Ms. Soumya Trivedi, AKG Engineering College, Ghaziabad

MEMBER-COORDINATOR

Dr. Munesh Chandra,

PSSCIVE, NCERT, Bhopal

Acknowledgement

On behalf of the 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 to the 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

UNIT 1
CYBER SECURITY

In the chapter-1 of this unit, you will explore the essential concepts of information security, starting with an introduction to its significance in protecting digital and physical data from unauthorized access and threats. You will learn about the CIA Triad, which consists of confidentiality, integrity, and availability—three core principles that guide security practices.

The chapter-2 of this unit will cover ethical hacking, where you'll understand how authorized professionals simulate attacks to identify vulnerabilities in systems. You'll gain insights into cryptography, learning how techniques like encryption and decryption secure communication and data.

In chapter-3, you will explore operating system security and access control mechanisms that protect data and manage user permissions. In chapter-4, an introduction to security tools for Windows OS will provide you with knowledge of software that helps defend against malware and unauthorized access.

In chapter-5, the course will cover wireless networks, including their types and security measures to safeguard them from various threats. **In chapter-6**, you will learn about mobile operating systems security aspects, specifically Android and iOS, examining their unique features, specializations, and the basic components of Android.

The chapter-7 will cover the realm of web applications, you will become familiar with key terminologies and browser security, alongside exploring web application protocols that govern data exchange over the internet. Additionally, you will discuss social media, including its advantages and disadvantages, and how to maintain security on these platforms.

In chapter-8, chapter-9 and chapter-10, You will also delve into digital payment systems, understanding their operation, security measures, and potential threats. The unit will introduce various types of banking fraud, helping you recognize and describe specific fraudulent activities. As you learn about cybercrime, you will gain an overview of cyber laws and the role of cyber cells in investigating these crimes. You will explore different classifications of cybercrime and cyber fraud, as well as the advantages of having established cyber laws to protect users and organizations. Finally, you will learn about the cyber fraud helpline system, which assists victims of cybercrime by providing support and resources to address their concerns.

By the end of this unit, you will have a comprehensive understanding of the various aspects of information security and the challenges presented by the digital landscape.

Chapter-1

Fundamentals of Cyber Security

Tanisha was diligently working on her school project, pouring hours into research and creative presentations. To keep her work safe, she saved all her files on her father's old laptop. One morning, she woke up excited to continue but found her files locked. There was a chilling message on the screen demanding money to unlock her precious work. Frightened and confused, Tanisha rushed to her father, who calmly explained that she had fallen victim to ransomware—a type of malware that encrypts files and demands a ransom for their release. He emphasized the importance of information security by backing up her data regularly and using reliable security software to prevent such incidents.

In this Chapter, you will learn about Introduction to Information Security, essential terminologies and its goals-CIA Triad.

1.1 Introduction to Information Security

The above story highlights how ransomware can disrupt everyday activities and teaches students the importance of being proactive in information security.

Information System

An information system is a combination of information technology equipment (Hardware & Software) and people's activities (using that technology) that supports operations, management, and decision-making in daily life (Figure 1.1).

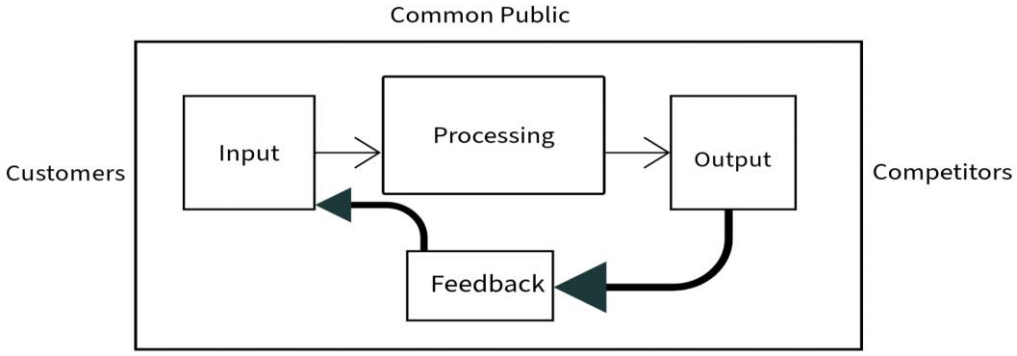


Figure 1.1 Information System Components

Information Security

Information security involves protecting information resources and information systems from unauthorized use, access, disclosure, modification, damage or destruction. Key characteristics of information security:

- It includes implementing strategies, policies, and technologies to safeguard data and systems.
- It aims to protect data from various threats, including cyberattacks, data breaches, and natural disasters, fostering trust and safety in information systems.
- It covers both physical security and cyber security of an information system.
- It is a methodological process not achieved by only applying certain tools.

1.2 Aspects of Information Security

A triangle diagram shown in Figure 1.2 effectively illustrates the relationship among three key information security aspects: usability, security, and functionality.

Usability

It is one corner of the triangle which is about how user-friendly the system is. If a system is easy to use, users can navigate it intuitively without needing extensive training or support.

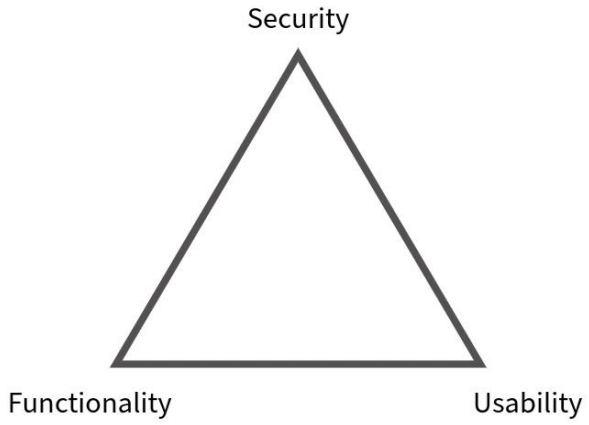


Figure 1.2 Security vs Functionality vs Usability

- **Importance**: If a system is difficult to use, users may abandon it, regardless of its security or functionality.

Security

The top corner of the triangle is about measures taken to protect systems against unauthorized access and data breaches. High security often requires stronger authentication measures and tighter access controls.

- **Importance**: Essential for maintaining trust. If a system is insecure, users may avoid it even if it's functional and user-friendly.

Functionality

The third corner of the triangle represents all the features and capabilities a system provides. The more functionality, the more tasks the system can perform.

- **Importance**: A system must perform well and meet user needs. However, excessive features can complicate usability and potentially introduce security risks.

Triangle Relationships

These three elements are interdependent. Focusing too much on one corner will tilt and imbalance the other two and improving one may impact the others as pointed below:

- **High Functionality**: It might complicate usability.
- **Strong Security**: It could limit functionality (e.g., more authentication steps).
- **User-Friendly Design**: It might overlook robust security measures.

The challenge is to find the right mix that aligns with your needs, ensuring the system is functional, user-friendly, and secure without compromising too much in any one area. When designing systems, aim for a balance among usability, security, and functionality. A triangle diagram visually represents this balance, showing that neglecting one aspect can compromise the overall effectiveness of the system.

Points to remember:

Information System-combination of hardware, software and its user's activities

Information Security-covers both physical and cyber security of an information system

Information Security Aspects-The challenge is to achieve balance among these three aspects

- **Usability-**The parameter to ensure how much easy to use the information system
- **Security-** The measures taken to protect systems against unauthorized access and data breaches
- **Functionality-**The more functionality, the more tasks the system can perform

1.3 Essential Terminologies for Information Security

Threat

An action, event, condition or circumstance that might prejudice and compromise security. A threat is a potential violation of security that causes harm or loss to an information system.

Example: Natural Disasters, Virus, Malware, Cyber Attacks

Risk

Probability of the occurrence of a threat is called risk.

Example: Risk of natural disasters, virus, malware and cyber attacks

Vulnerability

Existence of weakness in design or error in implementation of any information system that can lead to an unexpected, undesirable event compromising the security of the system.

Attack and Attacker

Attack is an assault on system security. It can be both active and passive. Attacker is an intruder, unethical and malicious person that performs an attack.

Exploit

It can be a tool, a software, or a technique that acts as a defined way to breach the security of the system through vulnerability. It takes advantage of vulnerabilities present in any information system.

Target Evaluation

An IT system, product, or component that is identified as requiring security evaluation.

Cyber Security

Cybersecurity is a field of practice for protecting systems, network infrastructures, network devices, and data from malicious attacks, unauthorized access, damage and prevent leakage of personal sensitive information. It includes a variety of tools, techniques, and best practices aimed at ensuring confidentiality, integrity, and availability of digital systems.

1.4 Information Security Goals

Apart from ensuring balance among security, functionality and usability, information security should achieve **C**onfidentiality, **I**ntegrity and **A**vailability-CIA triad, which is a universal goal of information security. The abbreviation CIA is formed from the first letter of these three words.

Confidentiality

Confidentiality ensures that sensitive information is accessed only by authorized users. This principle protects data from unauthorized access and breaches. While dealing with physical security of an information system, access control for confidentiality can be ensured by including security guards, alarms & locks and in case of cyber security Access controls for confidentiality are achieved by implementing user permissions and roles in software systems to restrict access to sensitive files. Encryption and decryption techniques are also used to restrict unauthorized access to an information system. Firewalls are also helpful in ensuring confidentiality.

Examples:

- Consider a Hospital Database which stores patient records electronically. Confidentiality is maintained by using encryption and access controls to ensure that only authorized medical staff & authority can view, use & edit patient information.
- Restricting access of financial records to the finance department personnel only.

Integrity

Integrity ensures that information is accurate and reliable, and that it has not been tampered or altered in any unauthorized manner. It guarantees that information is

accurate and complete, and protects it from unauthorized modification. Integrity can apply to physical paper documents or electronic ones. Checksums techniques, Hashing algorithms and Version Control tools are used to monitor whether the digital information has been modified or not. Integrity of information should be ensured in both states-on storage and while communication over networks.

Examples:

- Cryptographic Techniques like SHA-Secure Hash Algorithms are used to verify the integrity of data files. If a file's hash value matches the expected hash, it has not been altered.
- Version Control tools like Git track changes to files, allowing users to see edit history and restore previous versions if necessary.

Availability

Availability ensures that information and resources are accessible and available to authorized users when needed. Availability of an information system can be guaranteed by using redundant(backup) systems, regular hardware's maintenance and software updates to prevent downtime. Redundant (Backup Systems-like RAID-redundant array of inexpensive disks) or backup servers and data centers ensure that services remain operational even if one server fails. The availability of information systems which are connected to the internet are generally compromised by Distributed Denial of Service(D-DoS) attacks. Therefore, suitable strategies to prevent D-DoS attacks should be implemented.

Examples:

- An online banking system needs to be available 24/7 for customers to access their accounts.

By balancing these three principles, any organization can create a robust security framework to protect their information assets.

Points to remember:

Information Security Terminologies

- Threat
- Risk
- Vulnerability
- Attack and Attacker
- Exploit
- Target of Evaluation
- Cyber Security

Information Security Goals

The goal is to achieve Confidentiality, Integrity and Availability)-CIA triad.

- **Confidentiality-**ensures that sensitive information is accessed only by authorized users.
- **Integrity-** guarantees that information is accurate and complete, and protects it from unauthorized modification.
- **Availability-** Availability ensures that information and resources are accessible and available to authorized users when needed.

Practical Activity 1.1.

Objective: To learn about the need of information security by changing privacy settings on social media platforms.

Tools & Platform Needed:

- **Hardware:** Desktop/Laptop/Tablet/ Mobile Phone with internet
- **Apps:** Web Browser or any social media apps **(**e.g., Facebook, Instagram ,Whatsapp or Telegram).

Procedure:

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

Step 2. Assign each group a popular social media platform (e.g., Facebook, Instagram, Whatsapp or Telegram).

Step 3. Group leaders will create test accounts or use existing ones (with caution).

Step 4. All group members will explore and document various privacy settings of their assigned platforms.

Step 5. Group members will adjust privacy settings for maximum security.

Step 6. Each group will showcase their findings in form of presentation slides in front of class and discuss the importance of privacy settings and their impact on personal information security.

Practical Activity 1.2.

Objective: To understand importance of Data Backups for ensuring availability which is one of the information security CIA triad

Tools & Platform Needed:

- **Hardware:** USB, External Hard disks, Desktop/Laptop/Tablet/ Mobile Phone with internet
- **Apps:** Google Drive, Microsoft One Drive, any other cloud storage apps

Procedure:

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

Step 2. Instructor will present a scenario where important data is lost (e.g., computer crash, device lost).

Step 3. Instructor will discuss with learners about various backup options (cloud storage, external drives) and how they would restore or recover their files if data were lost.

Step 4. Assign each group USB Pendrive, External Hard Disks or any cloud storage platforms (e.g., Google Drive, Microsoft One Drive etc.).

Step 5. Learner's group will perform backup simulation to back up a sample file to a cloud platform, USB Pendrive, External Hard Drives

Step 6. All group members will explore and document various components of their assigned platforms.

Step 7. Each group will showcase their findings in form of reports or presentation slides in front of class and discuss the importance of back ups and availability.

List of other suggested practical activities:

- **Information Security News Discussion:** Follow and discuss recent cybersecurity news and incidents to stay informed about current threats.
- **Strong Password Making Exercise:** Create strong, unique passwords and test their strength using online tools.
- **Device Security Activity:** Set up screen locks and understand the significance of physical security for devices.
- Demonstrate the application of Information security (using imulator/Video) Demonstrate CIA Triad (using Simulator/Video)

SUMMARY

➔ Information System:

- Combines information technology (hardware & software) and people's activities.
- Supports operations, management, and decision-making.

➔ Information Security:

- Protects information systems from unauthorized use, access, disclosure, modification, damage, or destruction.
- Involves strategies, policies, and technologies to safeguard data and systems.
- Covers both physical security and cyber security.
- A methodological process, not achieved by only applying certain tools.

➔ Aspects of Information Security:

- Usability: User-friendliness of the system.
- Security: Measures to protect against unauthorized access and data breaches.
- Functionality: Features and capabilities of the system.
- These elements are interdependent, and balancing them is crucial.

➔ Essential Terminologies:

- Threat: Potential violation of security causing harm or loss.
- Risk: Probability of a threat occurring.
- Vulnerability: Weakness in design or implementation compromising security.
- Attack: Assault on system security.
- Exploit: Tool, software, or technique to breach security.
- Target Evaluation: Identifying systems requiring security evaluation.

➔ Cyber Security:

- Protects systems, networks, devices, and data from malicious attacks and unauthorized access.
- Ensures confidentiality, integrity, and availability of digital systems.

➔ Information Security Goals:

- Confidentiality: Restricting access to sensitive information to authorized users.
- Integrity: Ensuring information is accurate, reliable, and has not been tampered with.
- Availability: Ensuring information and resources are accessible to authorized users when needed.

By balancing these principles, organizations can create robust security frameworks to protect their information assets.

ASSESSMENT

A. Multiple Choice Questions

1. What is an Information System?
   a) A system combining information technology and people's activities.
   b) A system for storing physical documents.
   c) A system for processing only financial data.
   d) A system for controlling access to buildings.

2. What is the key characteristic of Information Security?
   a) Only applying certain tools.
   b) Implementing strategies, policies, and technologies.
   c) Ignoring physical security.
   d) Focusing solely on usability.

3. Which aspect of Information Security is about user-friendliness?
   a) Security
   b) Functionality
   c) Usability
   d) Confidentiality

4. What does the triangle diagram in Information Security illustrate?
   a) Relationship between usability, security, and functionality.
   b) Relationship between cost, time, and quality.
   c) Relationship between size, shape, and color.
   d) Relationship between speed, distance, and time.

5. What is a Threat in Information Security?
   a) A tool to improve security.
   b) A potential violation of security.
   c) A method to back up data.
   d) A type of network.

6. What ensures that information is accurate and reliable?
   a) Confidentiality
   b) Integrity
   c) Availability
   d) Usability

7. What is an Exploit in the context of Information Security?
   a) A tool, software, or technique to breach security.
   b) A method to update software.
   c) A type of encryption.
   d) A way to store data.

8. What is Cyber Security aimed at protecting?
   a) Physical documents
   b) Systems, networks, devices, and data
   c) Office furniture
   d) None of the above

9. What does Confidentiality ensure in Information Security?
   a) Data is accessed only by authorized users.
   b) Data is available to everyone.
   c) Data is modified frequently.
   d) Data is deleted regularly.

10. What is the purpose of Redundant (Backup) Systems?
    a) To reduce usability
    b) To ensure availability
    c) To decrease security
    d) To limit functionality

B. Fill in the Blanks

1. An Information System combines _____ technology and people's activities.
2. Information Security aims to protect information systems from unauthorized use, access, disclosure, _____ , damage, or destruction.
3. Usability, Security, and _____ are three key aspects of Information Security.
4. A Threat is a potential violation of security that causes harm or _____ to an information system.
5. The probability of a threat occurring is called _____.
6. Cyber Security protects systems, networks, devices, and data from malicious _____.
7. Confidentiality ensures that sensitive information is accessed only by _____ users.
8. Integrity ensures that information is accurate and _____.
9. Redundant systems help ensure the _____ of information and resources.
10. Firewalls are helpful in ensuring _____ by restricting unauthorized access.

C. True or False

1. An Information System is only made up of hardware.
2. Information Security includes both physical security and cyber security.

3. Usability is about how user-friendly a system is.
4. High functionality in a system can complicate usability.
5. Vulnerability refers to the existence of weakness in an information system.
6. An Exploit is a tool to back up data.
7. Cyber Security ensures the confidentiality, integrity, and availability of digital systems.
8. Confidentiality ensures that information is accessible to everyone.
9. Integrity guarantees that information has not been tampered with.
10. Availability ensures that information is accessible to authorized users when needed.

D. Short Answer Questions

1. What are the three key aspects of Information Security illustrated by the triangle diagram?
2. Define Vulnerability in the context of Information Security.
3. Explain the role of Redundant (Backup) Systems in ensuring availability.
4. What is the purpose of Two-Factor Authentication (2FA) in Cyber Security?
5. How do firewalls contribute to ensuring confidentiality in an information system?

E. Long Answer Questions

1. Discuss the relationship between usability, security, and functionality in Information Security. How can organizations balance these aspects?
2. Explain the CIA Triad (Confidentiality, Integrity, Availability) and its importance in Information Security. Provide examples for each principle.
3. Describe the key characteristics of Cyber Security and the tools and techniques used to protect systems, networks, devices, and data from malicious attacks.

ANSWER KEY

A. Multiple Choice Questions

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

B. Fill in the Blanks

1. information, 2. modification, 3. functionality, 4. loss, 5. risk, 6. attacks, 7. authorized, 8. consistent, 9. availability, 10. security

C. True or False

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

Chapter-2

Ethical Hacking and Cryptography

Tanu and her friends were wholeheartedly preparing for their final exams. Suddenly, they got to know that a mischievous unethical hacker had breached and attacked the School Board's server and downloaded the question papers and also shared it with a few students for some monetary gain. The multiple complaints were received by the school board from students and parents.

An ethical hacker was hired by the school board to audit their systems. While auditing, the ethical hacker identified suspicious activities on the server. He was able to trace the breach and identify the attackers, stopping the leakage of question papers further and reporting FIR against attackers to the nearest cyber crime cell. This story highlights the importance of ethical hacking, which helped in maintaining fairness and integrity in assessments. Tanu was now happy that the exam would be conducted in a fair manner. She and her friends thanked the ethical hacker silently.

In this Chapter, you will learn about Introduction to ethical hacking, essential terminologies and Cryptography basics.

2.1 Hacker, Cracker and Attacker:

Hacker

A hacker is a person skilled in computer programming, one who has a deep understanding of how computer systems and networks work. They can be ethical (white-hat hackers) who help improve security by finding and fixing vulnerabilities of organizations. Also, they can be unethical malicious(black-hat hackers) who do illegal hacking, often exposing vulnerabilities without permission.

Cracker

A cracker is an unethical, malicious, black-hat hacker who breaks into computer systems, software, or networks illegally causing damage or stealing of information. They

have malicious intentions, as they often bypass protections, such as passwords or encryption, to gain unauthorized access to apps, networks, or systems.

Example: A cracker can hack into an e-commerce website to steal customer credit card information and sell it on the deep web market.

Attacker

An attacker is a broader term as compared to crackers and hackers. Anyone who engages in illegal activities to compromise computer systems or networks, including malicious, unethical hackers, crackers and cybercriminals is called an attacker. Attackers may be highly skilled persons or an individual with basic knowledge of computer networks and systems. But their main purpose is to harm and gain access to the systems and resources illegally.

Example: Attackers launching ransomware on a city hospital, encrypting a database of patient personal records and critical illness details and demanding a ransom for its decryption.

2.1.1 Hacker Classes:

Black-Hats (Crackers or Malicious Hackers or Attackers)

These individuals with extraordinary computing skills are motivated to malicious or destruction activities. Their activities often include stealing data, causing damage and destruction, disrupting communication services, or gaining unauthorized access to any organization for getting sensitive information.

Example: A person who sends a lucrative phishing email to trap any organization's employee or common people into revealing personal information, such as passwords or organizations critical and sensitive details, is a black hat hacker.

White Hats (Ethical Hackers)

A **white-hat hacker** is an ethical hacker who may work for a company performing penetration testing and other security tests to find security flaws in its system. They are security analysts and cyber security experts for securing systems from attackers. White Hats claims to be knowledgeable about Black Hats activities. They can be consulting firms and former Black Hats.

Example: Ethical hackers at a company work to identify and fix vulnerabilities in servers, ensuring clients safety and help secure their systems from potential threats.

Gray Hats

Gray hat hackers play both roles ethical (white-hat) and malicious (black-hat) hackers. They are Crackers plus Hackers who do both offensive and defensive activity. They often hack into systems without permission but not with harmful intentions. Gray hat hackers intentions might not be malicious but their actions may be illegal.

Example: A hacker who finds a vulnerability in any organization's network infrastructure without permission but then informs the owners, expecting a reward or just for recognition.

Hacktivist and Hacktivism

Hacktivists are a group of hackers who perform cyberattacks to bring attention to issues like government corruption, organization's misconduct, human rights abuses, freedom of speech, or internet censorship. This activity and behaviour is collectively known as Hacktivism which is addressed as Hacking with/for a cause. They have a social or political agenda. They launch exploits for Distributed Denial of Service (DDoS) attacks, data leaks, and website defacement to bring the attention of the world.

Example:

1. Anonymous is one of the popular Hacktivist groups who raised their voice in the Black Lives Matter Campaign, following the murder of George Floyd in 2020. They hacked police departments sensitive information and communications of other institutions to expose and protest against police corruption and brutality
2. In 2016, WikiLeaks, exposed emails from Hillary Clinton's campaign, which was seen as a hacktivist act to expose political secrets and influence the United States Of America (USA) presidential election

2.1.2 Skills Required for Ethical Hacking:

An ethical hacking team performs a different set of security tests as a part of their job. Their team members must have different set of skill which are as follows:

Computer Networking Skills:

- Detailed idea about TCP/IP Protocol Suit working
- Knowledge of configuration of various networking devices such as routers, firewalls, intrusion detection systems(IDS), intrusion prevention systems (IPS) etc.
- Popular certifications from Cisco like CCNA Security, CCNP Security, CCIE Security

Programming Skills: C, C++, Python, HTML, JSP, PHP, SQL, Unix Shell scripting

Microsoft Based Systems Expertise: Microsoft Windows Client and Servers operations and configurations. Popular certifications from Microsoft like MCSA, MCSE.

Google and Android Based System Expertise: Google Chrome OS and Android OS operation and configurations.

Apple Based Systems Expertise: Operations and configuration of Apple Macintosh (MAC) operating system and iOS.

Linux/Unix OS Platforms: Knowledge of Linux/Unix operating system-based client and servers operations and configurations, Kali Linux operations OffSec Certified Professional (OSCP)- Penetration Testing with Kali Linux, RedHat Certification

EC-Council Certifications:

- CEH-Certified Ethical Hacker
- CPENT-Certified Penetration Testing Professional
- CHFI-Computer Hacking Forensic Investigator

Management Certifications: Apart from hacking stuff, evaluating and identifying vulnerabilities, an ethical hacker must have project management skills like planning, scheduling, executing and documenting security tests in a time bound manner. Project Management Certification (PMP) may be helpful for it.

Points to Remember:

Hacker-A hacker is a person with deep understanding of working of computer systems, programming and networks. They can be ethical (white-hat hackers) or unethical (black-hat hackers).

Cracker-A cracker is an unethical, malicious, black-hat hacker who breaks into computer systems, software, or networks illegally.

Attacker- Broder term all who engage in illegal activities to compromise systems. It includes hackers, crackers, and cybercriminals.

Hackers Classes-

- White-hats
- Black-hats
- Gray-hats
- Hactivists

Hacktivism-Hacking activity which is done to promote social causes or political agendas.

Skills Required to become an ethical hacker-

- Computer networking skills
- Computer Programming Skills
- Operating System Expertise

Certifications: CEH, CPENT, CHFI, PMP etc

2.2 A malicious hacker or an Attacker's Attacking Phases:

Any attacker or an malicious hacker goes through the following phases to launch an attack:

1. Reconnaissance
2. Scanning and Enumeration
3. Gaining Access
4. Maintaining Access
5. Covering Tracks

1. Reconnaissance

It is done by malicious hackers as an information gathering phase. It is done in two modes:

(i) Passive Reconnaissance

It involves sniffing and monitoring victims' network data for patterns and clues. It is done only on the local network and is not 100 % correct.

(ii) Active Reconnaissance

It involves probing and sniffing the network traffic to detect following things:

- ➔ Accessible hosts
- ➔ List of pen ports
- ➔ Location of routers
- ➔ Details of Operating Systems and Services

2. Scanning and Enumeration

It is also called pre-attack phase. Scanning helps hackers in identifying the weakness of the Information System. These are popular scanning techniques:

- ➔ Usage of dialers
- ➔ Network mapping
- ➔ Port Scanning
- ➔ Sweeping
- ➔ Usage of vulnerability scanners

The examples of popular scanning tools are Angry IP Scanner, Pinger, traceroute, Sweeper.

3. Gaining Access

It is the true attack phase. Attackers try to gain access over LAN, offline, locally, or the internet as a deception or theft. If the target system uses an outdated version of an application. Attackers could exploit a known vulnerability in that version to gain access. A hacker may discover an unpatched vulnerability in a web server, the hacker might use Metasploit to try exploiting it to gain administrative privileges opting any of the following techniques:

- ➔ Session Hijacking Attack

- ➔ Password Filtering Attack
- ➔ Buffer Overflows Attack
- ➔ Denial of Service Attack

4. Maintaining Access

Hacker tries to retain his ownership of the system. Hackers can upload, download or manipulate data, applications and set new configuration of the system. It helps in maintaining the connection and access to the target system for further exploitation and gathering more information or preparing for additional attacks if needed.They do system hardening with other hackers as well to own the system. System Hardening is done by applying following techniques:

Malware

virus, worm, Trojan Horse or Backdoors

Rootkits

It changes the behaviours of the critical binary of the system by debugging and releasing binary.

5. Covering Tracks

These are the activities undertaken by the hackers to extend his/her misuse of the system without being detected. His aim is to erase evidence of the hacking activities, ensuring the victims do not detect the attack. He plants rootkits, backdoors and clears logs and scripts to ensure no evidence of the attack is left behind.

2.3 Ethical Hacking Phases:

An ethical hacker and his team follows a systematic plan to detect and address vulnerability to prevent attacks of a malicious Hacker in a lawful manner. It is termed as ethical hacking phases which are as given below:

1. Granting Permission
2. Reconnaissance
3. Scanning and Enumeration
4. Gaining Access
5. Maintaining Access
6. Covering Tracks
7. Reporting
8. Training and Debrief

1. Granting Permission

First of all, an ethical hacker and his team first obtain a written permission. The phases they follow throughout their security tests are closely mapped with what a malicious hacker uses in attacks but ethical hacking is done with prior permission of the concerned organization.

2. Reconnaissance

It is an information gathering phase. An ethical hacker gathers as much information as possible about the target system or network. An ethical hacker might use tools like Nmap to scan for open ports and services running on the target server. He collects publicly available information about Organizations on social media, own and on other websites over the internet. Trace data leaks, which might lead to clues about organizations network vulnerabilities, personal information of key personnel, platforms and software used.

Suggested Tools: Nmap or WHOIS lookups to gather details about IP addresses and domains.

3. Scanning and Enumeration

It involves scanning the network traffic monitoring network data for patterns and clues to detect critical information like accessible hosts, open ports, location of routers, details of Operating Systems and Services. The popular scanning techniques are:

- Use of dialers
- Network mapping
- Port scanning
- Sweeping
- Usage of vulnerability scanners

Suggested Tools:

- Nessus or OpenVAS- vulnerability scanner
- Wireshark-analyze traffic for weak encryption or insecure protocols
- Angry IP Scanner
- Pinger
- traceroute
- Sweeper

4. Gaining Access

In this phase an ethical hacker launches an attack to check how an attacker can exploit identified vulnerabilities and gain unauthorized access to the target network infrastructure of the Organization. An ethical hacker may discover if there's an unpatched vulnerability in a web server or possibility of any outdated version of an application in the system.

Suggested Tools & Testing Techniques:

Usage of Metasploit to exploit a known vulnerability in a web application and systems with following techniques:

- Session Hijacking
- Password Filtering
- Buffer Overflows
- Denial of Service

5. Maintaining Access

Ethical Hacker maintains control of the system for outside access and restricts it for escalation of privilege by testing and uploading well known malware and backdoors. His team tests any possibility to change the behaviour and configuration of systems by launching rootkits. They ensure that the Production System (no compiler, no interpreter, IDE, Parser) must be different from the Development System.

Suggested Tools:

- Netcat- for launching backdoors for security test
- SELinux(Security Enhanced Linux)-Security-Enhanced Linux (SELinux) is a Linux kernel security module that helps protect the Linux operating system and kernel by implementing mandatory access control (MAC). SELinux is a set of kernel modifications and user-space tools that can be added to various Linux distributions.

6. Covering Tracks

Ethical hackers perform security tests to cover and uncover the tracks of malicious attacks.

Example: Usually organizations use layer 3 or layer 4 firewalls which block IP and Port addresses. It does not perform content checking that means to check modification in a log file with misleading entries. Ethical hackers fix their issue by installing application layer log monitoring tools, steganography based apps, tunneling (transfer and change the traffic like port traffic).

7. Reporting

Report writing is done within a week after completion of security testing by an ethical hacker. The report should include both technical and non-technical flaws in the network infrastructure of the organization. Remedies, recommendations and role wise preventive measures should be clear in the report.

8. Debrief & Training

Ethical hackers team provides debrief to technical and non-technical teams of organization based on their report finding. The client Organization can ask their queries and concerns during debrief. They conduct training and awareness sessions as per the needs of organizations.

Points to Remember:

Attacker Hacking Phase	Ethical Hacker Hacking Phase
• Reconnaissance (Information gathering) • Scanning and Enumeration: • Gaining Access • Maintaining Access. • Covering Tracks	• Granting Permission • Reconnaissance (Information gathering) • Scanning and Enumeration • Gaining Access • Maintaining Access:

		• Covering Tracks • Covering Tracks • Reporting • Training and Debrief

2.3 Security Tests by Ethical Hacker

Ethical Hacker performs a security test of the target of evaluation. The main purpose of security is to test for information gathering and identifying vulnerability in organization networks and infrastructures. Types of security tests are:

- **Black Box Testing:** with no prior knowledge of infrastructure to be tested
- **White Box Testing:** with a complete knowledge of network infrastructure to be tested
- **Gray Box Testing:** internal testing it examines extent of access by insiders within networks

2.3.1 Security Testing Modes in Ethical Hacking: After granting permission from the victim organization, an ethical hacking team may opt for any of the given security testing modes:

- **Local Network:** The first test the Local network for any loopholes and the vulnerability. The organization's local area networks are analyzed and attacked in a number of ways by an ethical hacking team.
- **Remote Network:** After the local network, organization's networks are attacked and accessed remotely for information gathering.
- **Wireless Network Testing:** The other aspect is assessing an organization's wireless network security. Methodology is mainly based on the type of wireless (WPA2-PSK/ WPA2 enterprise/guest) used in wireless devices which includes RFID-Radio Frequency Identification, Zigbee etc.
- **Penetration Testing:** This testing is popularly known as pen testing. The ethical hacking team simulates a set of cyber attacks on an organization's systems, networks and applications to identify and report available vulnerabilities. Pen Testing is done in two ways:
    - **Internal**-Assessing an organization's security from inside of the network. Methodology heavily focuses on active directory attacks
    - **External**-Assessing an organization's security from outside looking in.
- **Web Application Testing:** Assessing an organization's web application security. Methodology heavily focuses on web based attacks and OWASP(Open Web Application Security Projects) testing guidelines.
- **Authorization and Authentication Testing:** In this mode different accession rights and privileges of personnel are evaluated by an ethical hacking team. It estimates how much critical information is accessed and by whom.

- **Availability Testing or DoS Testing:** It is also called stress testing of the system against denial of service attack which compromises the availability of systems and servers.
- **Stolen Equipment:** The act of stealing critical electronic devices occurs occasionally in any organization to obtain crucial information. The same is tested by conducting a stolen equipment attack. The target may be any dignitaries of the organization.
- **Social Engineering:** It checks the integrity of the organization employees sending lucrative messages getting the organization's information. Activities include sending phishing mails, making phone calls and video calls to employees for getting organization's crucial information.
- **Physical Entry Testing:** Assessing an organization's physical security. Methodology mainly focuses on security goals and types of activities planned.
- **Cloud Security Testing:** This testing assesses vulnerability in cloud infrastructure of the Organization. All misconfiguration, data leakage and access are checked. SoutSuite, AWS Inspector are popular cloud security testing frameworks.
- **IOT Devices Security Testing:** It tests vulnerabilities in IOT devices which are being used in organization. Default id-passwords, APIs and encryption strengths are checked and evaluated. Tools like Shodan and IOT inspector may be tried by the testing team.
- **Compliance Testing:** It tests whether an organization follows and meets regulatory and security standards like PCI-DSS, GDPR etc. The compliance reports with corrective actions are produced as testing results.
- **Testing of Cyber Security and Communication Devices:** Firewall, IDS, IPS, Router, switches, PBX, VoIP, modems and many more devices are thoroughly tested for any loopholes, repair, upgradations and vulnerability.

Know more...

- **PCI-DSS** -The Payment Card Industry Data Security Standard is a set of guidelines and rules that protect credit card information

GDPR-The General Data Protection Regulation is a European Union (EU) law that protects the privacy and security of personal data

2.3.2. A Day in the life of an ethical hacker:

- Roll out of the bed
- Security Test Preparation
  - * formal contract
  - * non-disclosure agreement
  - * analyse pros and cons
- Perform Security Tests
- Write a report and Conclusion
- Give a debrief and training

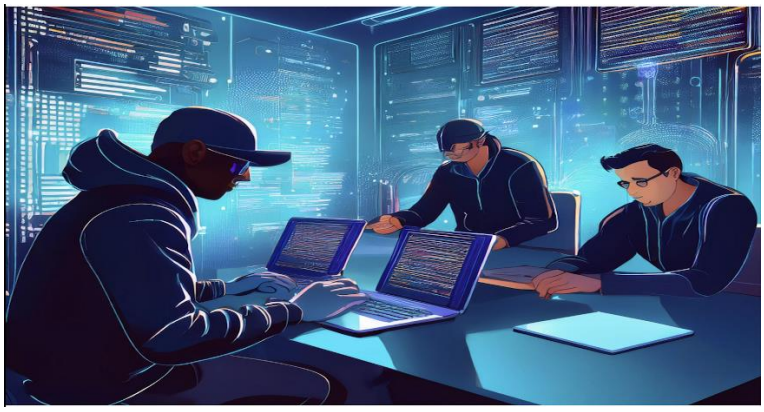


Figure 2.1 A day in the life of an ethical hacker with his team

Points to Remember:

Security Testing:

- Identify vulnerabilities in organization networks and infrastructures.

Types of Security Tests:

- Black Box Testing: No prior knowledge of the infrastructure.
- White Box Testing: Complete knowledge of the infrastructure.
- Gray Box Testing: Internal testing to assess insider access.

Security Testing Modes in Ethical Hacking:

- Testing on Local Network & Remote Network
- Wireless Network Testing
- Penetration Testing (Pen Testing)
- Web Application Testing
- Authorization and Authentication Testing
- Availability Testing (DoS Testing)
- Stolen Equipment Testing
- Social Engineering
- Physical Entry Testing
- Cloud Security Testing
- IoT Devices Security Testing
- Compliance Testing-PCI-DSS, GDPR.
- Testing of Cyber Security and Communication Devices

A Day in the Life of an Ethical Hacker:

- Perform security tests.
- Write a report and conclusion.
- Give a debrief and training.

2.4 Cryptography Overview:

Cryptography is defined as the process and study of techniques for securing information and communication from all except those who actually need it. The primary goals of cryptography are confidentiality, integrity, authentication, and non-repudiation. The two major processes in any cryptographic system are encryption and decryption.

Encryption

It involves converting information into a secure format termed as ciphers to protect information, ensuring confidentiality, integrity, and authenticity. Encryption is the process to convert plain text into cipher text using algorithms and keys. Encryption prevents unauthorized access to sensitive information.

Example: A message uses encryption before sending it over the internet ensures that only the intended recipient can read it.

Decryption

Decryption is the process of converting ciphertext back into plaintext using a decryption key.

Example: Receiving an encrypted email and using a private key to decrypt it and read the original message.

Important Terms used in Cryptography

Plain Text- It is readable text or any information

Cipher Text- Data which is not readable.

Cipher- A procedure or technique which is used in encryption and decryption. It is also called Cryptographic Algorithm.

Key- A piece of information used by a cipher to encrypt and decrypt data. It controls the functionality of cryptographic algorithms.

Public Key

In asymmetric-key cryptography, the key that can be shared publicly and is used to encrypt data.

Example: A public key is used to encrypt data that can only be decrypted by the corresponding private key.

Private Key

In asymmetric-key cryptography, the private key is kept secret and is used to decrypt data.

Example: A private key is used to decrypt data encrypted with the corresponding public key.

Digital Signature

A cryptographic technique that verifies the authenticity and integrity of a message or document.

Example: Signing an email with a digital signature ensures the recipient that the message has not been altered and confirms the sender's identity.

Hash Function

An algorithm that takes an input and produces a fixed-size string of characters, which appears random. It ensures data integrity by detecting changes to the original input.

Hash Functions converts data into a fixed-length hash value or digest.

It is Irreversible and used for verifying data integrity.

Example: SHA-256, Message Digest-5 (MD5).

Usage: Password storage, data integrity checks. SHA-256 (Secure Hash Algorithm 256-bit) is used to verify data integrity in blockchain transactions and digital signatures.

2.4.1 Role and Applications of Cryptography in Cyber Security

Cryptography plays a crucial role in ensuring the security and privacy of digital communications and data. Cryptography is the backbone of cybersecurity, ensuring the security of data in storage, transmission, and processing. It helps prevent unauthorized access, data breaches, and cyberattacks by securing communication networks in following ways:

1. **Achieving Confidentiality :**

   Cryptography can provide confidentiality. Data Encryption protects sensitive data (e.g., personal information, financial records) from being intercepted or accessed by malicious hackers or attackers.

   Example: Advanced Encryption Standard (AES) encryption is used to secure data over the internet. During sending an email, cryptographic algorithms like AES encrypt the message so that only the intended recipient with the decryption key can read it. Electronic Mail Services like Gmail and Outlook use encryption to protect users' emails.

2. **Achieving Integrity:**

   Integrity is that information remains unaltered from the point it is generated. Cryptography ensures secure communications and provides integrity and guarantees private and tamper-proof communication between sender and receiver.

   Example: When data is transmitted over the web, enabling HTTPS. HTTPS (HyperText Transfer Protocol Secure) uses SSL/TLS protocols. TLS/SSL protocols which incorporate cryptography to secure data transmitted between a user's browser and a website. This ensures that sensitive information like credit card details entered on an e-commerce site remains private.

   Secure Hash algorithms using Hash functions like SHA-256 ensure the integrity of data and verifies that it has not been tampered with.

3. **Achieving Authentication:** Cryptography helps in verifying the identity of users, systems, or devices to prevent unauthorized access.

Example: Digital signatures in email communication for sender verification. Cryptographic techniques, such as digital signatures, authenticate the sender's identity in digital communications. Digital certificates issued by Certificate Authorities (CAs) verify the authenticity of websites and software.

4. **Achieving Password Protection:** Cryptography supports storing user passwords securely using hashing algorithms.
5. **Cryptography in our day to day life:**
    - Maintaining privacy of phone calls, video calls
    - Popular messaging apps whatsapp, telegram uses end to end encryption
    - Popular Video Conferencing Apps Zoom, Google Meet, Microsoft Teams uses end to end encryption in their video communication
    - All Payments apps, Unified Payment System (UPI) uses secure online payments and transactions using cryptography.
    - Work from home online for a company using Virtual Private Network (VPN) which itself uses cryptography to secure data over public networks.

By incorporating cryptography into various cybersecurity preventive measures, organizations can safeguard their systems against various types of threats.

2.4.2 Types of Cryptography:

Symmetric-Key Cryptography:

It Uses the same single key for both encryption and decryption. Sender and receivers are assigned a pair of keys for encryption and decryption respectively (Figure 2.2).

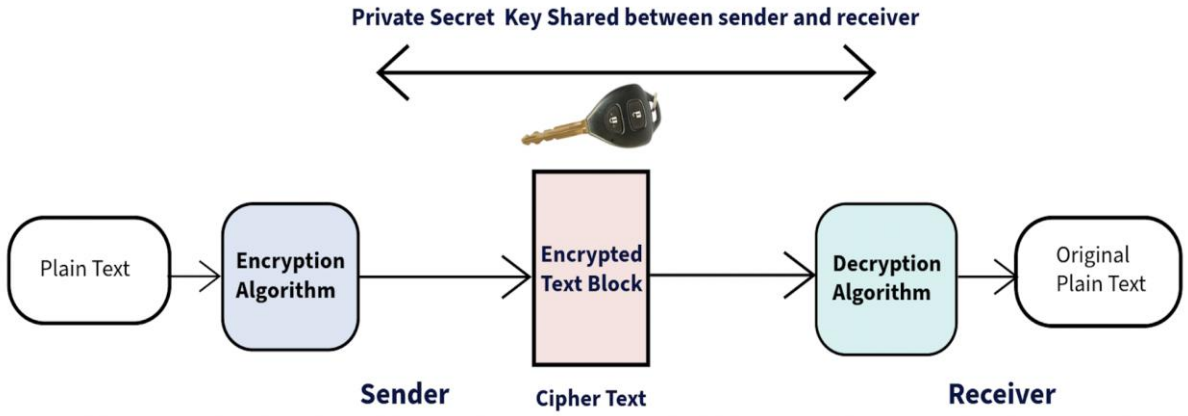


Figure 2.2 Symmetric Key Cryptography

Advantages:

It is faster and more efficient than asymmetric and suitable for encrypting large amounts of data.

Disadvantages:

(i) It requires secure key distribution.

(ii) It only provides confidentiality.

Example: Advanced Encryption Standard (AES), Data Encryption Standard (DES).

AES is a widely used symmetric-key encryption algorithm that secures data in various applications, including file encryption and secure file storage and communications between sender and receiver.

Asymmetric Key Cryptography:

It is also known as public key encryption. It differs from symmetric encryption in that it requires two keys. It uses a pair of keys—one public and one private. The public key encrypts data, while the private key decrypts it. The public key can be given to anyone, while recipients keep a private key for decryption (Figure 2.3).

Disadvantages:

(i) It is slower than symmetric.
(ii) It can provide confidentiality and authentication.

Example: RSA, Diffie-Hellman, ElGamal, and Elliptic Curve Cryptography (ECC) are asymmetric encryption algorithms. RSA (Rivest–Shamir–Adleman) is a common asymmetric algorithm used for secure data transmission over the internet, such as SSL/TLS for securing internet communications. The RSA cryptosystem is used in many applications, such as Microsoft Windows and Mozilla Firefox.

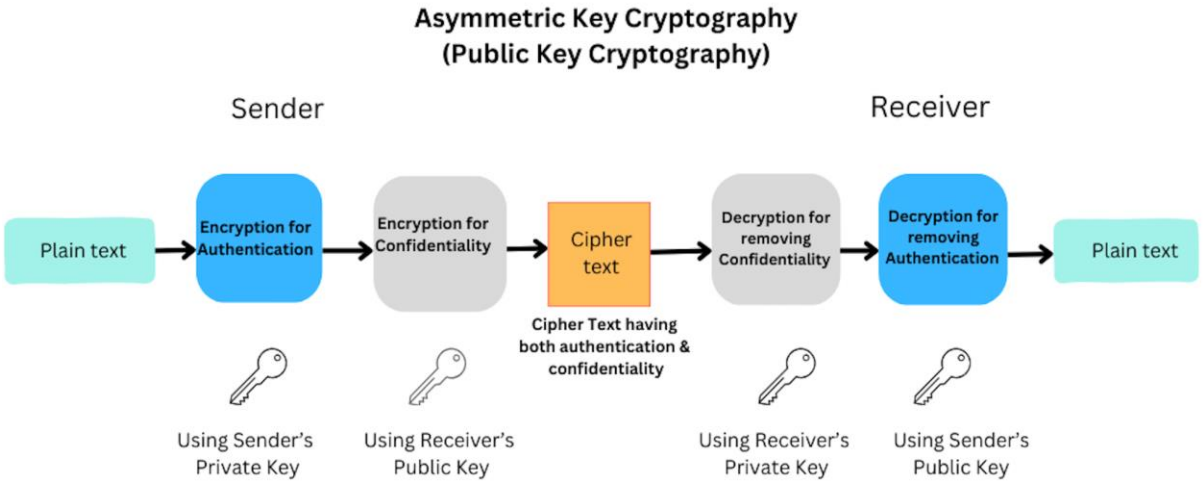


Figure 2.3 Asymmetric Key Cryptography ensuring both authentication and confidentiality

Know more...

Certificate Authority (CA)

An entity that issues digital certificates to verify the ownership of encryption keys used in secure communications. A CA is an organization that stores public keys and their owners. CAs are responsible for attesting to the identity of users, computers, and organizations. The CA's signature on a certificate allows users to easily detect tampering with the certificate's contents.

Example:

Godaddy-A CA that offers SSL certificates.

Digicert-A well-known CA that offers a wide range of digital certificates, including SSL/TLS, document signing, and code signing certificates.

Let's Encrypt: It is a CA that provides free SSL/TLS certificates for website encryption.

Vsign (Verasys): A licensed CA

eMudhra: The largest CA in India, eMudhra is licensed by the Government of India's Controller of Certifying Authorities. eMudhra offers digital certificates for a variety of needs, including income tax, banking, and foreign trade.

Safescrypt: A licensed CA

IDRBT: A licensed CA

CDAC: A licensed CA

Capricorn: A licensed CA

Protean (NSDL e-Gov): A licensed CA

Points to Remember:

Cryptography:

- The study and techniques of encryption and decryption for securing information and communication from unauthorized access.
- Goals: Confidentiality, integrity, authentication, and non-repudiation.
- Applications: End-to-end encryption in messaging apps, secure online payments, VPNs for remote work.
- Plain Text: Readable text or information.
- Cipher Text: Data in an unreadable format.
- Cipher: Technique used for encryption and decryption (Cryptographic Algorithm).
- Key: Information used by a cipher to encrypt and decrypt data.
- Public Key: Used to encrypt data, can be shared publicly.
- Private Key: Used to decrypt data, kept secret.
- Digital Signature: Verifies the authenticity and integrity of a message.
- Hash Function: Converts data into a fixed-length hash value; ensures data integrity. Hashing algorithms are used to store passwords securely.

Types of Cryptography:

Symmetric-Key Cryptography-Uses the same key for both encryption and decryption. Examples: AES, DES.

Asymmetric-Key Cryptography-Uses a pair of keys (public and private). Examples: RSA, Diffie-Hellman, ECC.

Practical Activity 2.1

Objective: Passive Information Gathering: Learners will learn how to gather information and identify vulnerabilities in a target system using reconnaissance and scanning techniques.

Tools & Platform Needed:

- Laptop or desktop computer with internet access

Group Formation and Task Assignment:

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

Step 2. Assign each group Passive Information gathering task for designated websites

Procedure to conduct Passive Reconnaissance:

Step 1. Use online tools such as WHOIS, WhatisMyIP, Shodan, and Google Dorking to gather information about the target system (e.g., IP addresses, domain names, server details).

Step 2: Document the process: Each group will showcase their findings in the form of presentation slides in front of class and discuss the importance of Passive Information Gathering.

Practical Activity 2.2

Objective: Active Information Gathering: Learners will learn how to gather information actively and identify vulnerabilities in a target system using reconnaissance and scanning techniques.

Tools & Platform Needed:

- Laptop or desktop computer with internet access
- Network scanning tools (e.g., Nmap)

Group Formation and Task Assignment:

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

Step 2. Assign each group Active Information gathering task for designated hosts.

Procedure to conduct Active Reconnaissance:

Step 1. Use Nmap to perform a network scan to identify live hosts, open ports, and services running on the target system.

Step 2. Run commands such as nmap -sP [target network range] to identify active hosts.

Step 3: Use nmap -sV [target IP] to determine the services and versions running on the target system.

Step 4: Document the process: Each group will showcase their findings in the form of presentation slides in front of class and discuss the importance of Active Information Gathering.

List of other suggested practical activities:

- **Social Engineering Role Play:** Conduct role-playing exercises where students attempt to gather information from their peers using social engineering techniques. This helps them understand the human element of security.
- **Network Analysis:** Demonstration of tools like Wireshark and usage of tools to analyze the types of data transferred over network. Download Link: https://www.wireshark.org/download.html
- **Basic Cryptography Activity:** Perform encryption & decryption using online or offline tool

SUMMARY

Hacker:

- Skilled in computer programming with deep understanding of systems and networks.
- White-Hat Hackers: Ethical, help improve security by finding and fixing vulnerabilities.
- Black-Hat Hackers: Unethical, perform illegal hacking to exploit vulnerabilities.

Cracker:

- Unethical, malicious black-hat hacker.
- Breaks into systems illegally to cause damage or steal information.
- Example: Hacking an e-commerce website to steal customer credit card information.

Attacker:

- Broader term encompassing all who engage in illegal activities to compromise systems.
- Includes hackers, crackers, and cybercriminals.
- Example: Launching ransomware on a hospital to demand ransom for encrypted data.

Hacker Classes:

- Black-Hats: Malicious activities like stealing data and causing damage.
- White-Hats: Ethical hackers performing security tests and fixing vulnerabilities.
- Gray Hats: Both ethical and malicious, often hack without harmful intentions but may act illegally.
- Hacktivists: Hack to promote social or political agendas, e.g., Anonymous group.

Skills Required for Ethical Hacking:

- Networking Skills: Knowledge of TCP/IP, routers, firewalls, IDS, IPS.
- Programming Skills: Proficiency in languages like C, C++, Python, HTML, SQL.
- System Expertise: Familiarity with Microsoft, Google, Android, Apple, Linux/Unix OS.
- Certifications: CEH, CPENT, CHFI, PMP.

Attacking Phases:

- Reconnaissance: Information gathering, passive (monitoring) and active (probing).
- Scanning and Enumeration: Identifying system weaknesses using tools like Angry IP Scanner.
- Gaining Access: Exploiting vulnerabilities to access systems (e.g., session hijacking).
- Maintaining Access: Uploading, downloading, manipulating data, and hardening systems.
- Covering Tracks: Erasing evidence of hacking activities to avoid detection.

Purpose of Security Testing:

- Identify vulnerabilities in organization networks and infrastructures.

Types of Security Tests:

- Black Box Testing: No prior knowledge of the infrastructure.
- White Box Testing: Complete knowledge of the infrastructure.
- Gray Box Testing: Internal testing to assess insider access.

Security Testing Modes in Ethical Hacking:

- Local Network: Analyzing and attacking local area networks.
- Remote Network: Remotely accessing and attacking networks for information gathering.
- Wireless Network Testing: Assessing wireless security based on the type of wireless used (e.g., WPA2-PSK, RFID, Zigbee).
- Penetration Testing (Pen Testing): Simulating cyber attacks to identify vulnerabilities, conducted internally or externally.
- Web Application Testing: Assessing security of web applications using OWASP guidelines.
- Authorization and Authentication Testing: Evaluating access rights and privileges of personnel.
- Availability Testing (DoS Testing): Stress testing systems against denial of service attacks.
- Stolen Equipment Testing: Simulating theft of critical devices to test information security.
- Social Engineering: Testing integrity of employees by sending phishing emails and making deceptive calls.
- Physical Entry Testing: Assessing physical security of the organization.
- Cloud Security Testing: Assessing vulnerabilities in cloud infrastructure.
- IoT Devices Security Testing: Testing vulnerabilities in IoT devices.
- Compliance Testing: Ensuring adherence to regulatory and security standards like PCI-DSS, GDPR.
- Testing of Cyber Security and Communication Devices: Checking firewalls, IDS, IPS, routers, and other devices for vulnerabilities.

A Day in the Life of an Ethical Hacker:

- Perform security tests.
- Write a report and conclusion.
- Give a debrief.

Cryptography:

- The study and techniques for securing information and communication from unauthorized access.
- Goals: Confidentiality, integrity, authentication, and non-repudiation.
- Key processes: Encryption (converting plain text into cipher text) and Decryption (converting ciphertext back into plain text).

Important Terms:

- Plain Text: Readable text or information.
- Cipher Text: Data in an unreadable format.
- Cipher: Technique used for encryption and decryption (Cryptographic Algorithm).
- Key: Information used by a cipher to encrypt and decrypt data.
- Public Key: Used to encrypt data, can be shared publicly.
- Private Key: Used to decrypt data, kept secret.
- Digital Signature: Verifies the authenticity and integrity of a message.
- Hash Function: Converts data into a fixed-length hash value; ensures data integrity.

Role and Applications of Cryptography in Cyber Security:

- Confidentiality: Protects data from unauthorized access (e.g., AES encryption).
- Integrity: Ensures information remains unaltered (e.g., HTTPS using SSL/TLS).
- Authentication: Verifies user identities (e.g., digital signatures).
- Password Protection: Uses hashing algorithms to store passwords securely.
- Daily Applications: End-to-end encryption in messaging apps, secure online payments, VPNs for remote work.

Types of Cryptography:

➔ **Symmetric-Key Cryptography:**

- Uses the same key for both encryption and decryption.
- Advantages: Faster and efficient.
- Disadvantages: Requires secure key distribution.
- Examples: AES, DES.

➔ **Asymmetric-Key Cryptography:**

- Uses a pair of keys (public and private).
- Advantages: Easy key exchange.
- Disadvantages: Slower than symmetric.
- Examples: RSA, Diffie-Hellman, ECC.

ASSESSMENT

A. Multiple Choice Questions

1. Who is a White-Hat Hacker?
   a) An unethical hacker who exploits vulnerabilities.
   b) An ethical hacker who helps improve security.
   c) A hacker who breaks into systems illegally.
   d) None of the above.

2. What is a Cracker?
   a) A person who tests software.
   b) An ethical hacker.
   c) An unethical hacker who breaks into systems to cause damage or steal

information.
d) A cybersecurity expert.

3. What term encompasses all who engage in illegal activities to compromise systems?
   a) Hacker
   b) Cracker
   c) Attacker
   d) None of the above.

4. Which of the following is a skill required for ethical hacking?
   a) Cooking skills
   b) Knowledge of TCP/IP, routers, firewalls, IDS, IPS
   c) Musical skills
   d) Gardening skills

5. What phase involves information gathering in hacking?
   a) Gaining Access
   b) Reconnaissance
   c) Covering Tracks
   d) Maintaining Access

6. What type of security test involves no prior knowledge of the infrastructure?
   a) White Box Testing
   b) Gray Box Testing
   c) Black Box Testing
   d) Penetration Testing

7. Which mode of security testing involves assessing wireless security based on the type of wireless used?
   a) Local Network Testing
   b) Remote Network Testing
   c) Web Application Testing
   d) Wireless Network Testing

8. What is the purpose of Compliance Testing?
   a) To break into systems.
   b) To test the physical security of an organization.
   c) To ensure adherence to regulatory and security standards.
   d) To steal information.

9. What does cryptography aim to achieve?
   a) Making information unreadable.
   b) Securing information and communication from unauthorized access.
   c) Deleting data.
   d) Printing information.

10. Which cryptographic technique uses a pair of keys (public and private)?
    a) Symmetric-Key Cryptography
    b) Asymmetric-Key Cryptography
    c) Hash Functions
    d) Digital Signatures

B. Fill in the Blanks

1. A _____ is skilled in computer programming with a deep understanding of systems and networks.
2. _____ is an unethical hacker who breaks into systems illegally to cause damage or steal information.
3. _____ is a broader term encompassing all who engage in illegal activities to compromise systems.
4. Black-Hat hackers perform _____ activities like stealing data and causing damage.
5. _____ hackers often hack without harmful intentions but may act illegally.
6. An ethical hacker must have networking skills, including knowledge of _____.
7. The phase of hacking that involves information gathering is called _____.
8. _____ Testing involves analyzing and attacking local area networks.
9. Cryptography aims to achieve confidentiality, integrity, authentication, and _____.
10. _____ uses the same key for both encryption and decryption.

C. True or False

1. Black-Hat hackers are ethical hackers.
2. A cracker is an unethical, malicious black-hat hacker.
3. An attacker includes hackers, crackers, and cybercriminals.
4. White-Hat hackers perform security tests and fix vulnerabilities.
5. Gray Hat hackers are always ethical.
6. Reconnaissance is the phase where vulnerabilities are exploited.
7. Black Box Testing involves complete knowledge of the infrastructure.
8. Penetration Testing simulates cyber attacks to identify vulnerabilities.
9. Cryptography ensures data remains unaltered, which is called integrity.
10. Asymmetric-Key Cryptography uses a pair of keys for encryption and decryption.

D. Short Answer Questions

1. What is the difference between a hacker and a cracker?
2. Describe the role of a White-Hat hacker.
3. What are the skills required for ethical hacking?

4. Explain the purpose of penetration testing.
5. How does cryptography contribute to cybersecurity?

E. Long Answer Questions

1. Discuss the phases of an attack conducted by a malicious hacker. Provide examples for each phase.
2. Compare and contrast Symmetric-Key Cryptography and Asymmetric-Key Cryptography, including their advantages and disadvantages.
3. Explain the various security testing modes used by ethical hackers. How do these modes help in identifying vulnerabilities in an organization's infrastructure?

ANSWER KEY

A. Multiple Choice Questions

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

B. Fill in the Blanks

1.Hacker, 2.Cracker, 3.Attacker, 4.Illegal, 5.Gray Hat, 6.TCP/IP, 7.Reconnaissance, 8.Local Network, 9.Non-repudiation, 10.Symmetric-Key Cryptography

C. True or False

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

Chapter-3

Operating System Security

Aarav, a Windows Operating System user, thought he had taken all the necessary precautions to secure his computer, but one day his worst fears came true. He had downloaded software on his Windows OS, but unknown to him, it was malware. The malware hacked into his computer and stole his sensitive data. He soon discovered that his bank account and credit card information had been compromised. Aarav immediately notified his bank and credit card company, but the damage was already done. He felt helpless and violated, wondering how this could have happened to him.

This experience taught Aarav the importance of having security tools for Windows OS. He realized that antivirus software and firewalls are not just optional features, but essential components of computer security. Aarav installed reputable antivirus software and enabled the firewall on his Windows OS. He also started using strong, unique passwords for all his online accounts and enabled two-factor authentication whenever possible.

Aarav hopes his story serves as a warning to others. Don't make the same mistake he made. Take the necessary steps to secure your computer and protect your digital life. Install security tools, use strong passwords, and stay vigilant.

This chapter explores the key concepts of OS security, focusing on access control, User Accounts, File Permissions, Password Policies, and Log Management.

3.1 Operating System Security

Operating system (OS) security is a crucial aspect of any system performance and a critical one as per cybersecurity point of view, as the OS acts as an intermediary between the user and the hardware. It provides an interface between computer user and computer hardware. It manages hardware as well as other systems and applications software resources by enforcing security policies. Operating system security aims to safeguard the system's core functions, applications, and user data from unauthorized access, breaches,

and other cyber threats. Effective OS security measures protect the system from unauthorized access, ensure data integrity, confidentiality and maintain system stability with availability.

- Confidentiality: Ensuring only authorized users can access data.
- Integrity: Preventing unauthorized modification of data.
- Availability: Ensuring systems and data are available to its legitimate user when needed.

Since the OS controls everything on a device, securing it is very important. Weak security can lead to:

- Unauthorized access
- Data theft
- Malware and viruses
- System damage

3.2 Role of Access Control in OS Security

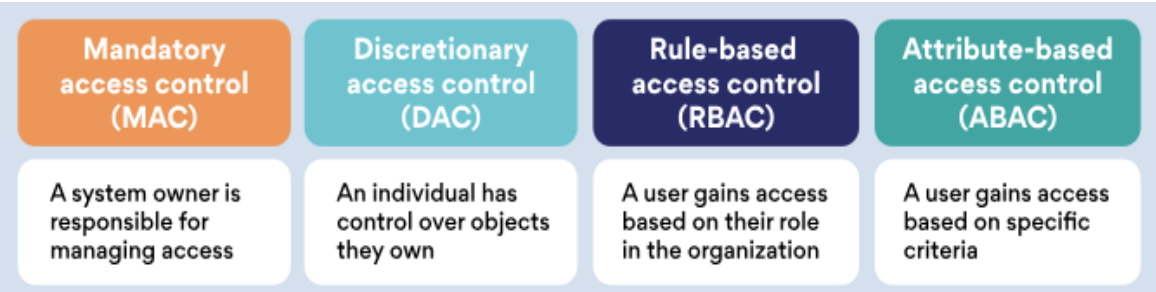
Access control is a very important component and critical factor of OS security that determines who or what can view or use resources in an Operating System working environment. It is essential for protecting sensitive information and ensuring that only authorized users can perform specific actions and access the data.

Access Control means deciding who can access what in the system. Access Control helps in creating security mechanisms for any operating system. It controls how users, applications, and processes interact with system resources like files, directories, memory and all hardware devices connected with Operating System.

3.2.1 Key Factors of Access Control:

- **Authentication**
  Authentication verifies the identity of a user or process using credentials like passwords, biometric data, or security tokens.
- **Authorization**
  Authorization determines the permissions granted to authenticated users, specifying what actions they can perform on resources.

Types of Access Control



1. Discretionary Access Control (DAC):

In DAC, the resource owner decides who can access it and what permissionsthey have. This type of control is flexible but can be less secure if not managed properly.

Example: A user who creates a file can set permissions to allow other users to read, write, or execute the file.

2. Mandatory Access Control (MAC):

In MAC, the access control Policies are independent of resource ownership.It is a stricter access control model where access policies are determined by a central authority and cannot be altered by individual users. It is often used in government and military applications.

Example: Classified information systems where users are granted access based on their security clearance level.

3. Role-Based Access Control (RBAC): In RBAC, permissions are assigned based on user roles within the organization. It simplifies management by grouping users with similar access needs.

Example: An organization may have roles such as "Manager" and "Employee," with each role having specific permissions to access resources.

4. Attribute-Based Access Control (ABAC):

ABAC uses attributes (resource type, time, duration, specific event, environment conditions) to determine access permissions. It offers fine-grained control and flexibility.

Example: Access to a document may be granted based on the user's department, the time of day, duration, and the sensitivity level of the document.

- **Windows**: Uses "User Accounts" and "Permissions".

  Example: A student user cannot install software without Admin rights.
- **Android**: Uses "App Permissions". Example: Camera permission must be given to apps like WhatsApp.
- **Linux**: Uses "User IDs (UIDs)" and "Groups" to control access.

3.2.2 File Access Control

Windows OS provides granular control over files and folders through permissions. Granular control allows administrators to define precise access permissions for users and groups, based on their role, need, or other attributes. Granular control can be applied to a variety of systems, including: databases, apps, pages, web servers, software, systems, and files. Every file/folder has permissions that control:

- **Read (R)** → Who can view the file
- **Write (W)** → Who can change the file
- **Execute (X)** → Who can run a program

Windows: Right-click a file → *Properties* → *Security Tab* → set permissions for users.
Android: Android uses App sandboxing. Each app has isolated storage. Apps access files only if permission is given. Example: A photo editor app can only open pictures if allowed.

Linux: It uses the *chmod* command.

Example:

```
chmod 755 myfile.txt
```

It gives full access to the owner, and read-execute to others.

Granular control is important for protecting sensitive data and mitigating the risk of data breaches and insider threats. It ensures that users only have access to the information they need for their role, and that sensitive information is only accessible to authorized individuals. There are different types of file access control permissions such as :

- Full Control: Read, write, execute, and modify permissions.
- Modify: Read and write but no control over permissions.
- Read & Execute: View and execute files without modifications.

Points to Remember:

Operating system (OS) security protects against unauthorized access, data breaches, and cyber threats. It ensures confidentiality, integrity, and availability of system resources.

Access Control in OS Security restricts unauthorized access to system resources.

Access control components:

- Authentication: Verifies user identity.
- Authorization: Defines permissions for authenticated users.

Access Control Models:

- Discretionary Access Control (DAC): resource owners control permissions.
- Mandatory Access Control (MAC): permissions enforced by policies.
- Role-Based Access Control (RBAC): permissions assigned based on roles.
- Attribute-Based Access Control (ABAC): permissions based on user attributes.

3.3 User Accounts and Policies

Purpose of User Accounts

- Secure Multi-User Access: User accounts enable multiple individuals to use the same device while keeping their data, settings, and permissions separate and secure.

User Account Control (UAC)

UAC prevents unauthorized changes to the OS by prompting for administrative credentials when critical actions are performed.

Account Types

- Administrator / Root:
  - Has full control over the system.
  - Can install software, change system settings, manage other user accounts, and access all files.
- Standard User:
  - Has limited access.

- Can use installed applications and modify personal settings but cannot make system-wide changes or manage other accounts.

Key Policies

- Individual Accounts for Each User:
  - Ensures accountability and personalized settings.
  - Prevents unauthorized access to another user's data.
- Strong Passwords Required:
  - Protects accounts from unauthorized access.
  - Should include a mix of letters, numbers, and symbols.
- Disable Guest Accounts:
  - Guest accounts often lack password protection and can be exploited.
  - Disabling them enhances overall system security.

3.4 User Account Creation and Management

Windows

- Where to Create Accounts:
  - Use Control Panel → User Accounts or
  - Settings → Accounts.
- Who Can Manage:
  - Only Administrators can add or remove user accounts.
- Why It Matters:
  - Helps tailor access levels and keeps each user's data separate and secure.

Android

- Multi-User Support:
  - Found under Settings → System → Multiple users.
- Account Types:
  - Supports standard users and guest accounts.
- Use Case:
  - Ideal for shared devices like tablets, allowing personalized experiences without compromising privacy.

Linux

- **Account Creation:** New users are created using terminal commands.

```bash
sudo adduser student1
```

- **Admin Controls:**
  - Admins can assign users to specific groups and define permissions.
- **Flexibility:**
  - Offers granular control over system access and resource usage.

Key Point:

Proper account management is essential to:

- Prevent unauthorized access
- Protect personal and sensitive data
- Ensure smooth multi-user operation across devices

3.5 Password Policies

Passwords are the first line of defense against unauthorized access. A strong password policy helps:

- Protect user accounts and sensitive data
- Prevent brute-force and credential-stuffing attacks
- Promote responsible user behavior and system hygiene2

Core Password Requirements

- Minimum Length:
  - Passwords should be at least 8 characters long.
  - Longer passwords (12–14+ characters) are recommended for better security.
- Character Complexity:
  - Use a mix of:
    - Uppercase letters (A–Z)
    - Lowercase letters (a–z)
    - Numbers (0–9)
    - Symbols (!, @, #, etc.)
  - This increases entropy and makes passwords harder to guess.
- Avoid Common Passwords:
  - Never use predictable patterns like “12345”, “password”, or “admin”.
  - These are easily cracked and often targeted by attackers.
- Regular Changes:
  - Periodically update passwords to reduce the risk of long-term exposure.
  - However, forced frequent changes can lead to weaker passwords due to user fatigue.
- No Reuse of Old Passwords:
  - Reusing passwords across accounts or recycling old ones increases vulnerability.
  - Each password should be unique and not based on previous ones.

Platform-Specific Enforcement

Windows

- Administrators can enforce password policies using:
  - Local Security Policy (secpol.msc)
  - Group Policy Editor (gpedit.msc)

- Settings include:
    - Minimum password length
    - Complexity requirements
    - Password expiration and history

Android

- Offers multiple authentication methods:
    - PIN, Password, Pattern Lock
    - Biometric options like fingerprint and facial recognition
- Users can choose based on convenience and security level

Linux

- Password policies are configured in:
    - /etc/login.defs for system-wide rules
    - /etc/pam.d/ for Pluggable Authentication Modules (PAM)
    - Linux uses *passwd* and *chage* commands.
- Admins can set:
    - Minimum length
    - Password aging (expiration)
    - History and reuse restrictions

Tips for Strong Password Hygiene

- Use passphrases: e.g., “BlueSky!RunsFast2025”
- Consider a password manager to store and generate secure passwords
- Enable multi-factor authentication (MFA) wherever possible
- Avoid sharing passwords via email or chat

3.6 Operating System Log Management

What Are Logs?

Logs are chronological records of system events, activities, and errors generated by the operating system (OS) and applications. They serve as a vital tool for:

- Monitoring system health
- Troubleshooting issues
- Detecting security breaches
- Auditing user activity

3.6.1 Windows Logs

- **Tool Used**: **Event Viewer**
- **Types of Logs**:

    - **Security Logs**: Track login attempts, account access, and permission changes.
    - **Application Logs**: Record errors and warnings from installed software.
    - **System Logs**: Capture OS-level events like driver failures or service crashes.
- **Use Case**: Admins can detect suspicious login attempts, software malfunctions, or unauthorized access.

3.6.2 Android Logs

- **Access Method**: Developers use tools like **Logcat** via Android Studio or ADB (Android Debug Bridge).
- **Log Categories**:
    - **System Logs**: OS-level operations and hardware interactions.
    - **App Logs**: Debugging messages, crashes, and performance metrics.
- **Use Case**: Essential for app debugging and performance tuning. Can also reveal system-level anomalies.

3.6.3 Linux Logs

- **Storage Location**: /var/log/ directory
- **Key Log Files**:
    - **auth.log or secure:** Tracks authentication attempts (e.g., SSH logins).
    - **syslog:** General system messages.
    - **dmesg:** Kernel-related messages.
    - **boot.log:** Startup sequence logs.
- **Use Case**: Admins can monitor failed login attempts, system errors, and service status.

Real-World Example

If someone tries to **break into a system**, the OS will record the **failed login attempts** in its logs.

- On **Windows**, this appears in the **Security log** via Event Viewer.
- On **Linux**, it's captured in auth.log.
- On **Android**, developers may spot anomalies in **Logcat output**.

Why Logs Matter for Security

Logs record system activities and help detect suspicious behavior. It helps in:

- **Intrusion Detection**: Spot brute-force attacks or unauthorized access.
- **Incident Response**: Reconstruct events leading to a breach.
- **Compliance**: Meet regulatory requirements for data protection and auditing.
- **Performance Monitoring**: Identify bottlenecks or failing components.

Practical Activity 3.1

Objective: Understanding User Account Types and Permissions

Tools & Platform Needed:

- Windows/Linux computer
- Admin access

Group Formation and Task Assignment:

Step 1: Divide students into pairs.

Step 2: Assign each pair a system to explore user accounts and permissions.

Procedure:

Step 1: Open the user account settings (Control Panel in Windows or terminal in Linux).

Step 2: Create a new Standard User account.

Step 3: Attempt to install software or change system settings using the Standard User account.

Step 4: Switch to Administrator/Root account and repeat the same actions.

Step 5: Document differences in access and control.

Step 6: Present findings and explain why limiting user privileges enhances security.

Practical Activity 3.2

Objective: Monitoring System Logs for Security Events

Tools & Platform Needed:

- Windows/Linux/Android device

Group Formation and Task Assignment:

Step 1: Form groups of 3 students.

Step 2: Assign each group a platform to explore logs.

Procedure:

Step 1: On Windows, open Event Viewer → Security logs.

Step 2: On Linux, access /var/log/auth.log or syslog.

Step 3: On Android (developer mode), use Logcat to view logs.

Step 4: Identify login attempts, errors, or suspicious activity.

Step 5: Document findings and explain how logs help in detecting threats.

List of other suggested practical activities:

1. **Objective:** Exploring File Access Control

   Tools & Platform Needed:

- Windows/Linux computer
- Sample files

2. **Objective:** Implementing Strong Password Policies

Tools & Platform Needed:

- Windows/Linux/Android device
- Internet access

3. **Objective:** Exploring Access Control Models

Tools & Platform Needed:

- Chart paper or digital presentation tools
- Internet access for research

SUMMARY

Operating system security is vital for maintaining system performance and protecting against cyber threats. As the OS manages hardware and software resources, it must enforce robust security policies to safeguard core functions, applications, and user data.

Core Security Principles

- **Confidentiality:** Only authorized users can access data.
- **Integrity:** Prevents unauthorized data modification.
- **Availability:** Ensures systems and data are accessible to legitimate users when needed.

Weak OS security can lead to:

- Unauthorized access
- Data theft
- Malware infections
- System damage

Access Control in OS Security

Access control defines who can view or use system resources, ensuring sensitive data is protected.

Key Components:

- **Authentication:** Verifies identity using passwords, biometrics, or tokens.
- **Authorization:** Grants permissions based on user roles or attributes.

Types of Access Control:

Type	Description
DAC	Users control access to their own resources
MAC	Access is enforced by system policies
RBAC	Permissions based on user roles
ABAC	Access based on attributes like department, time, or sensitivity

- **Windows:** User accounts and permissions
- **Android:** App permissions
- **Linux:** User IDs and groups

File Access Control

Granular control over files and folders ensures only authorized users can read, write, or execute files.

Permission Types:

- **Read (R):** View content
- **Write (W):** Modify content
- **Execute (X):** Run programs

Platform-Specific Controls:

- **Windows:** Security tab in file properties
- **Android:** App sandboxing and permission requests
- **Linux:** chmod command (e.g., chmod 755 myfile.txt)

Granular access control helps prevent data breaches and insider threats.

User Accounts and Policies

Purpose:

- Enables secure multi-user access
- Separates user data and permissions

Account Types:

- Administrator / Root: Full system control
- Standard User: Limited access

Key Policies:

- Individual Accounts: Ensures accountability
- Strong Passwords: Mix of characters for security
- Disable Guest Accounts: Prevents misuse due to lack of protection

Additional Feature:

- User Account Control (UAC) in Windows prompts for admin credentials during critical actions to prevent unauthorized changes.

User Account Creation and Management

- **Windows**: Accounts created via Control Panel or Settings; only admins can manage users.
- **Android**: Supports multiple users and guest accounts under Settings → System.
- **Linux**: Users created via terminal; admins assign groups and permissions.
- **Key Point**: Proper account management prevents unauthorized access and protects personal data.

Password Policies

- **Strong Passwords**: Minimum 8 characters, mix of cases, numbers, and symbols.
- **Avoid Weak Passwords**: No “12345” or “password”.
- **Change Regularly**: Avoid reuse; update periodically.

- **Platform Enforcement**:
  - **Windows**: Enforced via Local Security Policy and Group Policy Editor.
  - **Android**: Offers PIN, password, pattern, and biometrics.
  - **Linux**: Uses /etc/login.defs, PAM, passwd, and chage.
- **Tips**: Use passphrases, password managers, and enable MFA.

Operating System Log Management

- **Purpose**: Logs track system events, errors, and security activities.
- **Windows**: Event Viewer logs security, application, and system events.
- **Android**: Developers use Logcat for system and app logs.
- **Linux**: Logs stored in /var/log/ (e.g., auth.log, syslog, dmesg).
- **Security Role**: Logs aid in intrusion detection, incident response, compliance, and performance monitoring.

ASSESSMENT

A. Multiple Choice Questions

1. What does NTFS stand for?
   (a) New Technology File System
   (b) Network Transfer File System
   (c) Native Text File System
   (d) None of the above

2. In Windows, user accounts are managed via:
   (a) Terminal
   (b) Control Panel
   (c) Registry
   (d) BIOS

3. What does chmod 700 file.txt do?
   (a) Everyone can read
   (b) Only owner has full access
   (c) No one can access
   (d) File is deleted

4. Android logs can be viewed using:
   (a) Event Viewer
   (b) Logcat
   (c) Task Manager
   (d) Registry Editor

5. Which command changes a user's password in Linux?
   (a) passwd
   (b) usermod
   (c) chpass
   (d) changepwd

6. In which type of access control can the owner of the resource set permissions?
   (a) Discretionary Access Control (DAC)
   (b) Mandatory Access Control (MAC)
   (c) Role-Based Access Control (RBAC)
   (d) Attribute-Based Access Control (ABAC)

7. What is the primary objective of access control in OS security?
   (a) Speed up processing
   (b) Prevent unauthorized access
   (c) Increase network traffic
   (d) Reduce system logs

8. Which of these is not an access control model?
   (a) DAC
   (b) RBAC
   (c) MAC
   (d) TAC

9. Android uses which method for access control?
   (a) NTFS
   (b) App sandboxing
   (c) chmod
   (d) Registry

10. Which policy helps prevent brute-force attacks?
    (a) Password length
    (b) Account lockout
    (c) File permission
    (d) Log rotation

B. Fill in the blanks:

1. In Role-Based Access Control, permissions are assigned based on _____.
2. The _____ model assigns access permissions based on user attributes.
3. The primary goal of _____ in OS security is to restrict unauthorized access.
4. UAC stands for _____.
5. In the RBAC model, permissions are assigned based on _____.
6. _____ Access Control allows resource owners to define access permissions.
7. The command to add a user in Linux is _____.
8. Android uses _____ to isolate apps.
9. Windows uses _____ for file permissions.
10. Linux stores logs in the _____ directory.
11. _____ is used to view logs in Android.
12. Event Viewer is used to view logs in _____.

13. The command to change a password in Linux is _____.
14. Account lockout policy helps prevent _____.
15. _____ is used to enforce security settings in Windows.

C. True or False

1. Role-Based Access Control assigns permissions based on individual user discretion.
2. Mandatory Access Control allows users to set their own access permissions.
3. Discretionary Access Control is based on a central authority setting access policies.
4. Android supports multiple user accounts.
5. NTFS is a file system used in Linux. → False
6. chmod is used in Linux to change file permissions.
7. Windows uses Event Viewer for log management.
8. Android apps share the same storage space.
9. Linux uses /etc/login.defs for password policies.
10. File permissions help control access to files.
11. Log files are useful for detecting security breaches.
12. Windows does not support password policies.

D. Short Answer type questions.

1. What is the purpose of User Account Control (UAC)?
2. Define Role-Based Access Control (RBAC).
3. What is access control in operating systems?
4. How does Android manage app permissions?
5. What is the purpose of password policies?
6. Name two commands used for user management in Linux.
7. Why is log management important?

E. Long Answer type questions.

1. Discuss the importance of operating system security and how access control models contribute to it.
2. Explain the different types of access control models and their applications in OS security.
3. Explain how file permissions work in Windows, Android, and Linux with examples.
4. Describe the process of creating and managing user accounts in Linux.
5. Discuss the importance of log management and how it differs across Windows, Android, and Linux.

ANSWER KEY

A. Multiple Choice Questions

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

B. Fill in the Blanks

1.roles, 2.Attribute-Based Access Control (ABAC), 3.access control, 4.User Account Control, 5.roles, 6.Discretionary, 7.useradd, 8.app sandboxing, 9.NTFS, 10./var/log, 11.Logcat, 12.Windows, 13.passwd, 14.brute-force attacks, 15.Group Policy

C. True or False

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

Chapter-4

Security Tools for Windows OS

Utkarsh, a freelance graphic designer from Mumbai, used his Windows laptop for work. He spent most of his time designing logos, brochures, and websites for clients. Utkarsh thought he was safe from cyber threats since he didn't store sensitive information like passwords or credit card numbers on his laptop.

One day, while working on a project, Utkarsh clicked on a suspicious link sent by an unknown email address. Unaware to him, the link downloaded malware onto his laptop. The malware slowly started taking control of his system, allowing hackers to access his files and personal data.

Utkarsh's laptop started behaving strangely. His files were getting deleted, and his antivirus software was not detecting any threats. It was then that he realized his laptop had been compromised. Panicked, Utkarsh immediately disconnected his laptop from the internet and sought help from a cybersecurity expert.

The expert told Utkarsh that his laptop was infected with ransomware, which had encrypted his files, making them inaccessible. Utkarsh had to pay a ransom in cryptocurrency to get the decryption key. However, there was no guarantee that the hackers would provide the key even after receiving the payment.

Utkarsh learned a valuable lesson about the importance of cybersecurity. He realized that having reliable antivirus software and a firewall was not enough. He needed more advanced security tools to protect his Windows laptop from sophisticated cyber threats.

Utkarsh's story highlights the importance of having advanced security tools to protect Windows laptops from cyber threats.

Security Tools available in Windows OS

Windows OS has various built-in security tools designed to protect the system from threats and vulnerabilities and enhance security. These tools work together to provide overall security and protection from threats like malware, unauthorized access, and data breaches.

4.1 Windows Firewall

Windows Firewall is a network security application that monitors and controls incoming and outgoing network traffic based on predefined inbound and outbound security rules. It blocks unauthorized access to the system and permits safe communication among different applications and networks.

Key Features:

- **Inbound and Outbound Filtering:** Controls both inbound and outbound traffic to prevent unauthorized access.
- **Application Blocking**: Blocks or allows applications from accessing the network based on user-defined rules.
- **Customizable Settings:** Allows users to create custom rules and profiles to meet specific security needs.

Example: Windows Firewall can be configured to block all incoming connections except those necessary for essential services, enhancing the system's security.

4.1.1 Configuring Windows Firewall Settings

To effectively use Windows Firewall, it's essential to understand how to configure its settings.

Here's a step-by-step guide to managing Windows Firewall settings:

- Accessing Windows Firewall Settings:
  - Go to Control Panel > System and Security > Windows Defender Firewall.

    See Figure 4.1 and 4.2.

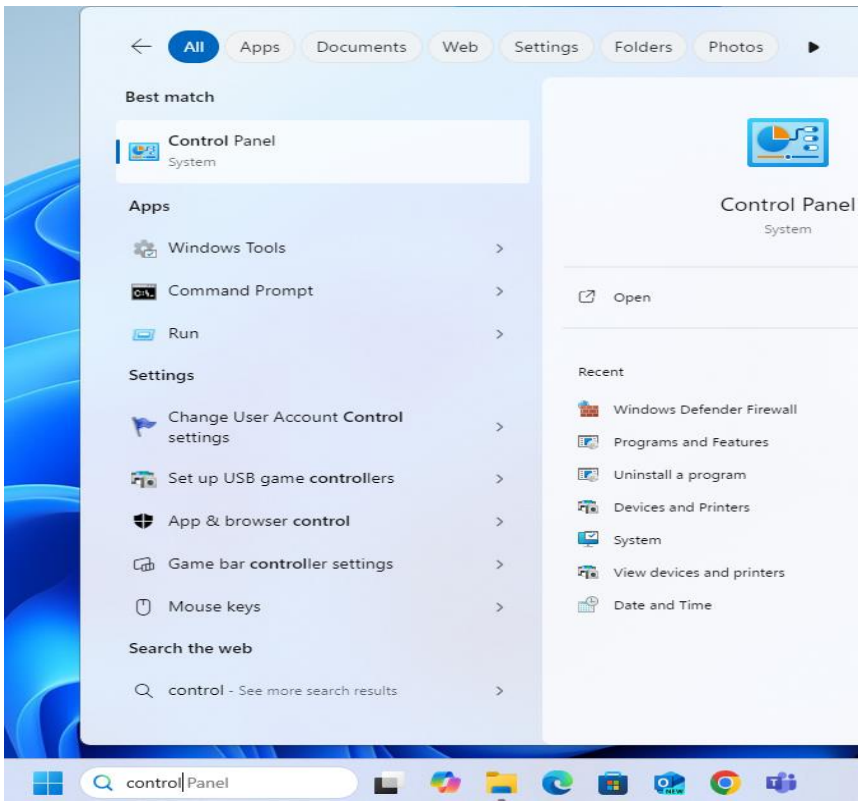


Figure 4.1 Accessing Windows control panel

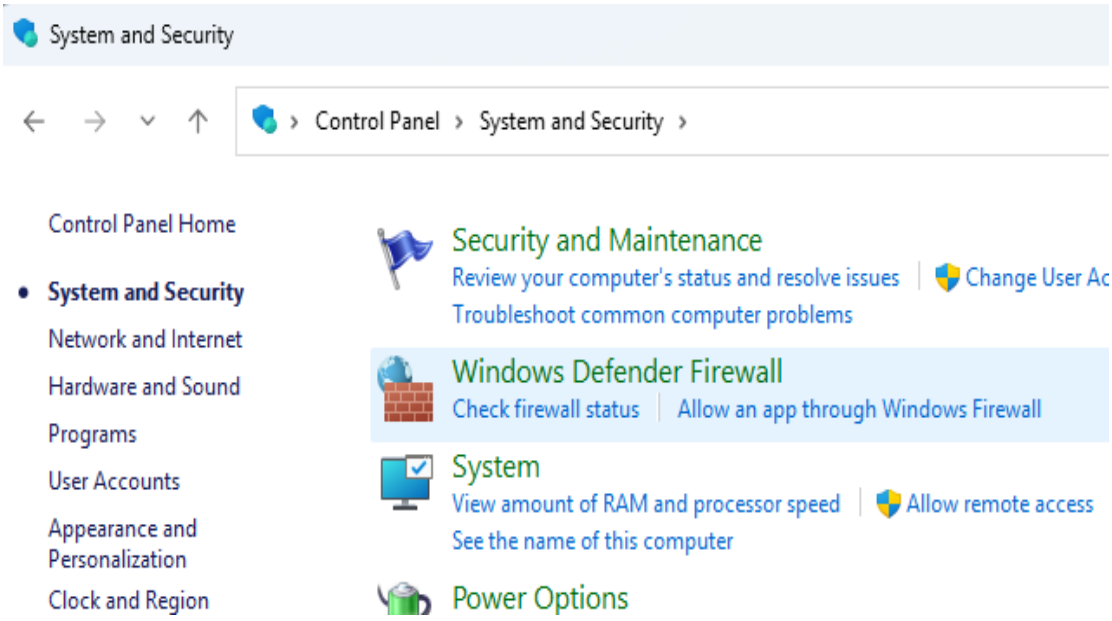


Figure 4.2 Accessing Windows Defender Firewall

- Click on Advanced settings to open the Windows Firewall with the Advanced Security console. (Figure 4.3 and 4.4)

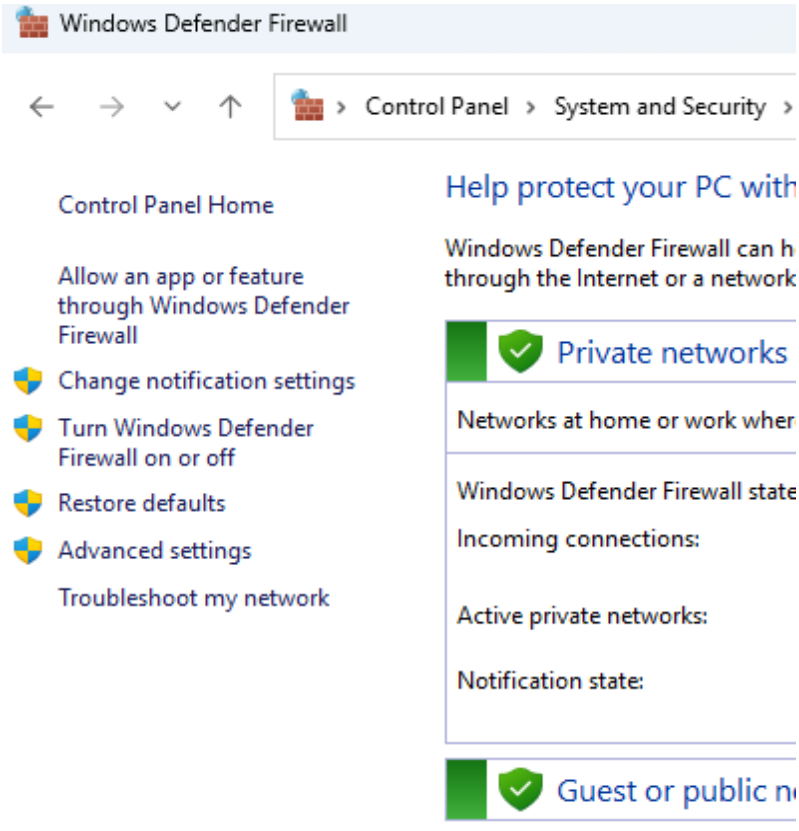


Figure 4.3 Accessing Advanced Setting option of Windows Defender Firewall

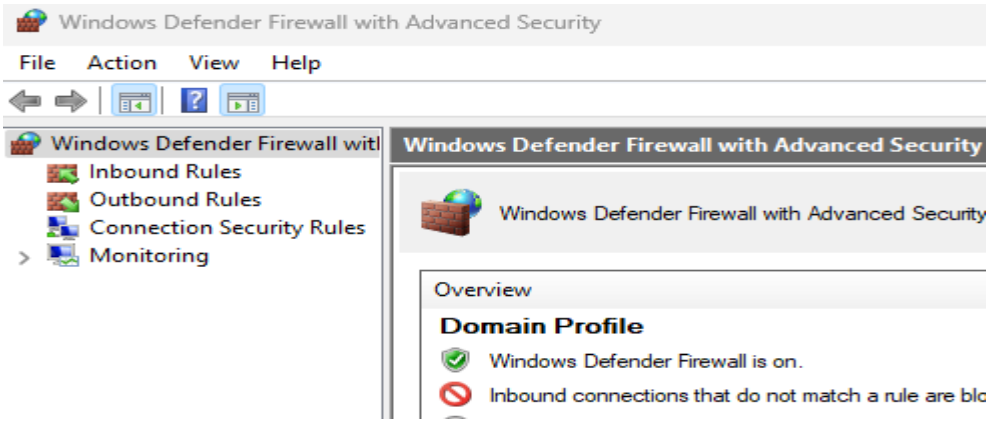


Figure 4.4 Accessing Advanced Security Console of Windows Defender Firewall

- Creating Inbound Rules:
  - In the left pane, click on Inbound Rules.
  - In the right pane, click on New Rule. (Figure 4.5 and 4.6)

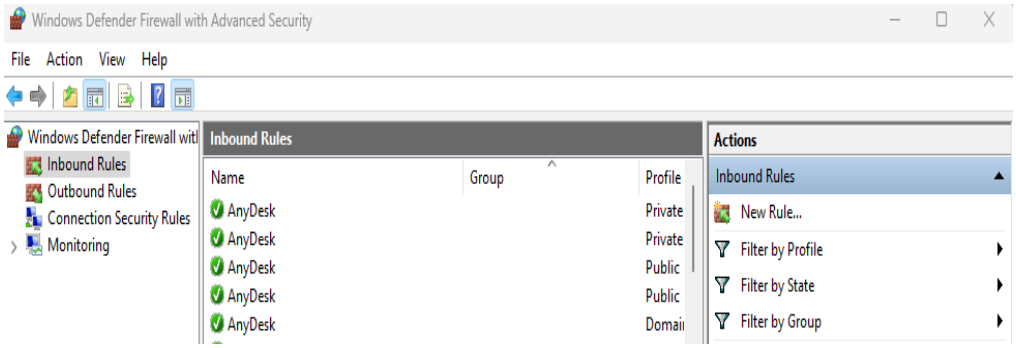


Figure 4.5 Accessing Inbound Rules of Windows Defender Firewall

  - Choose the rule type (e.g., Program, Port).

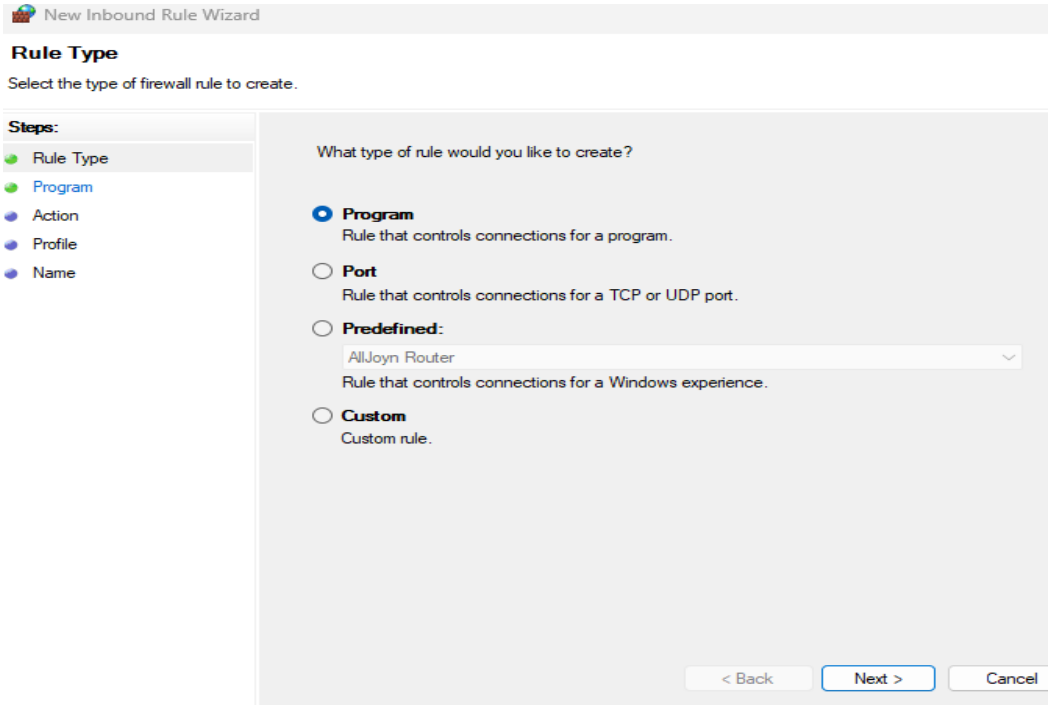


Figure 4.6 Configure new Inbound Rules for Windows Defender Firewall

- Follow the prompts to specify the program or port, action (allow or block), and profile (Domain, Private, Public). (Figure 4.7-4.9)

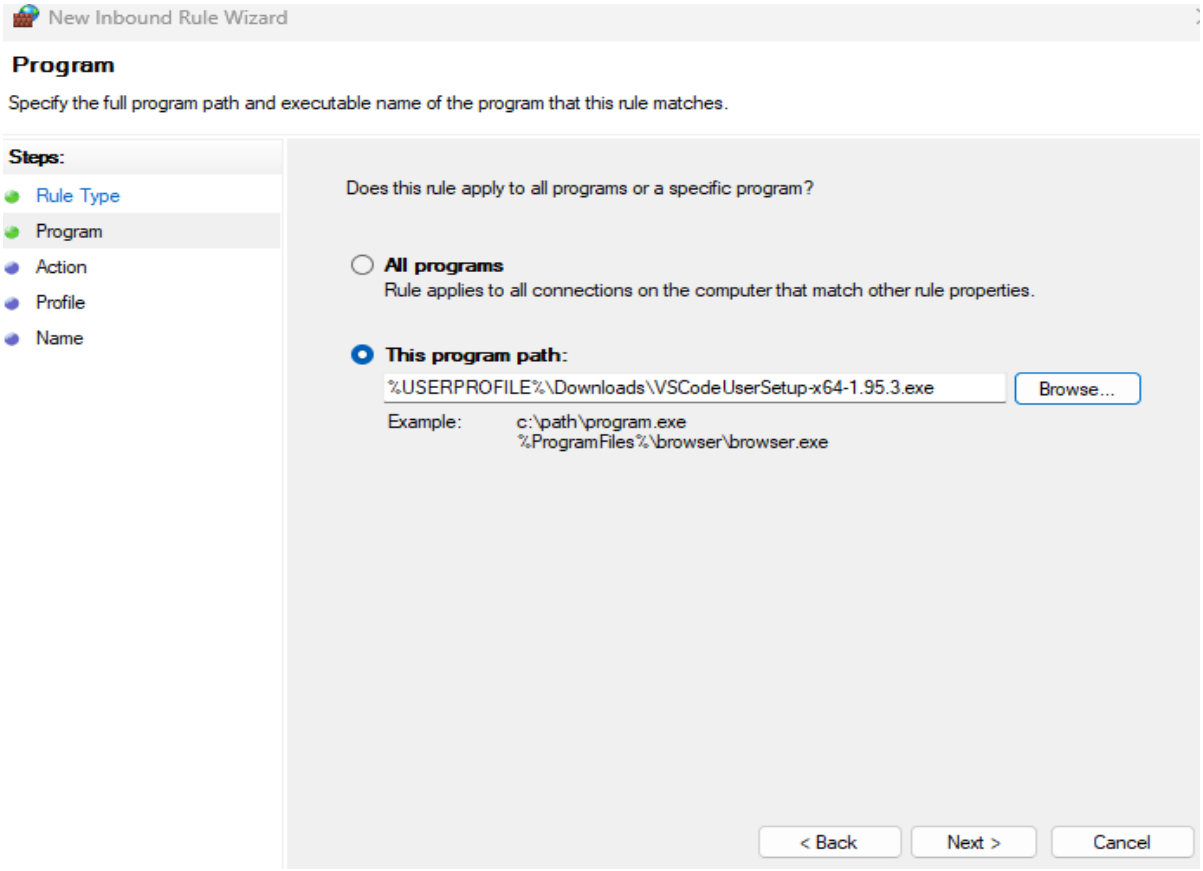


Figure 4.7 Configure path of new Inbound Rules for Windows Defender Firewall

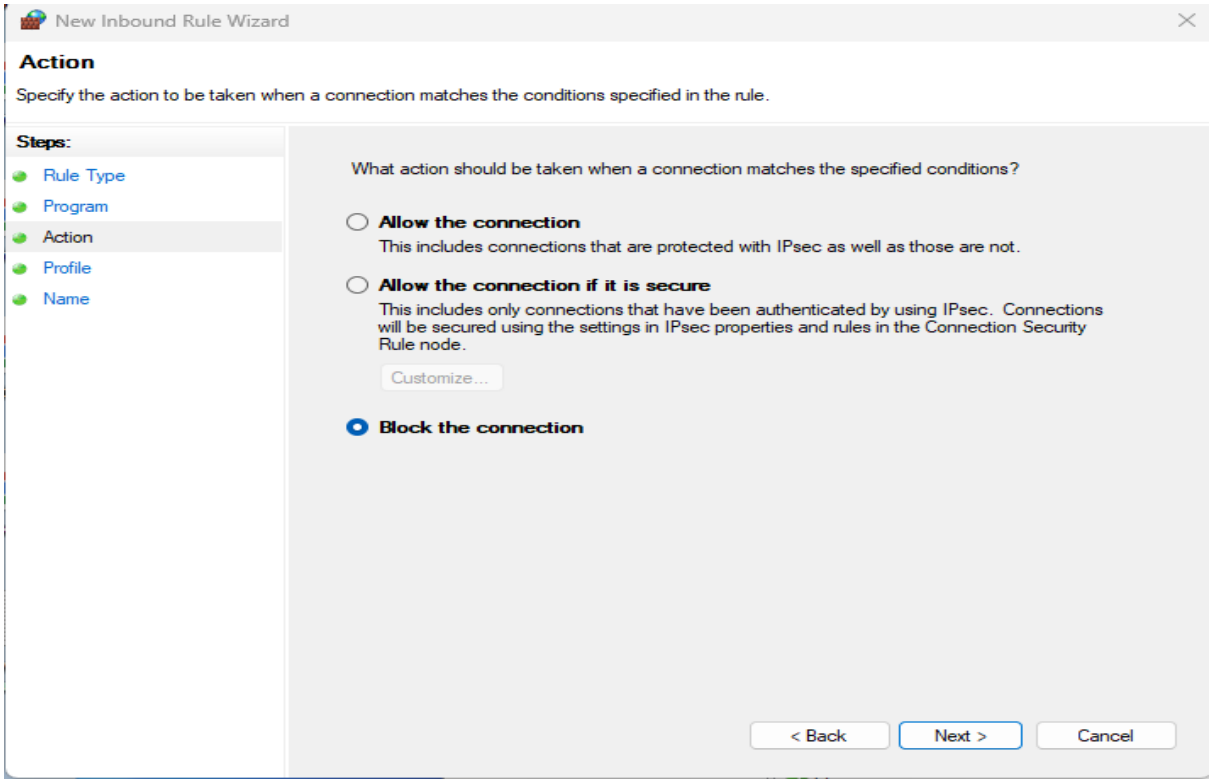


Figure 4.8 Configure action of new Inbound Rules for Windows Defender Firewall

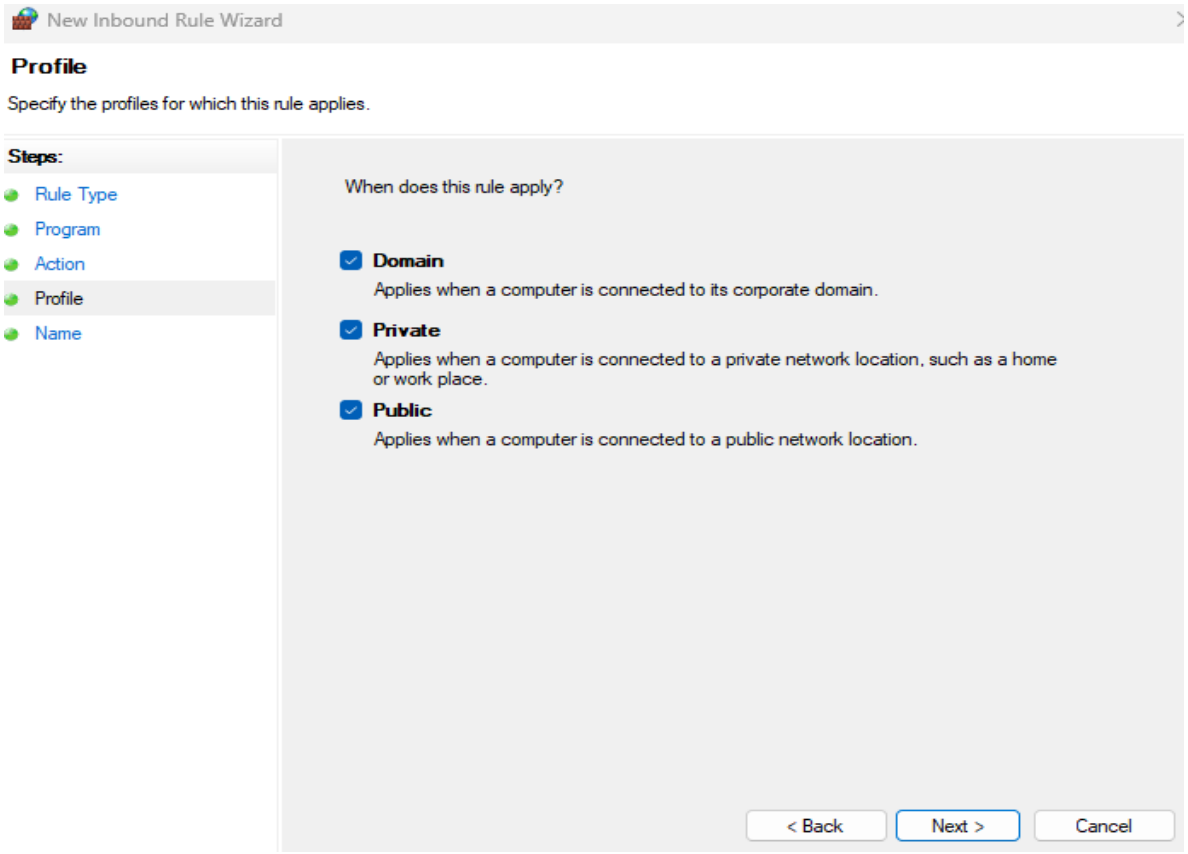


Figure 4.9 Configure Profile of new Inbound Rules for Windows Defender Firewall

- Name the rule and click Finish. (Figure 4.10)

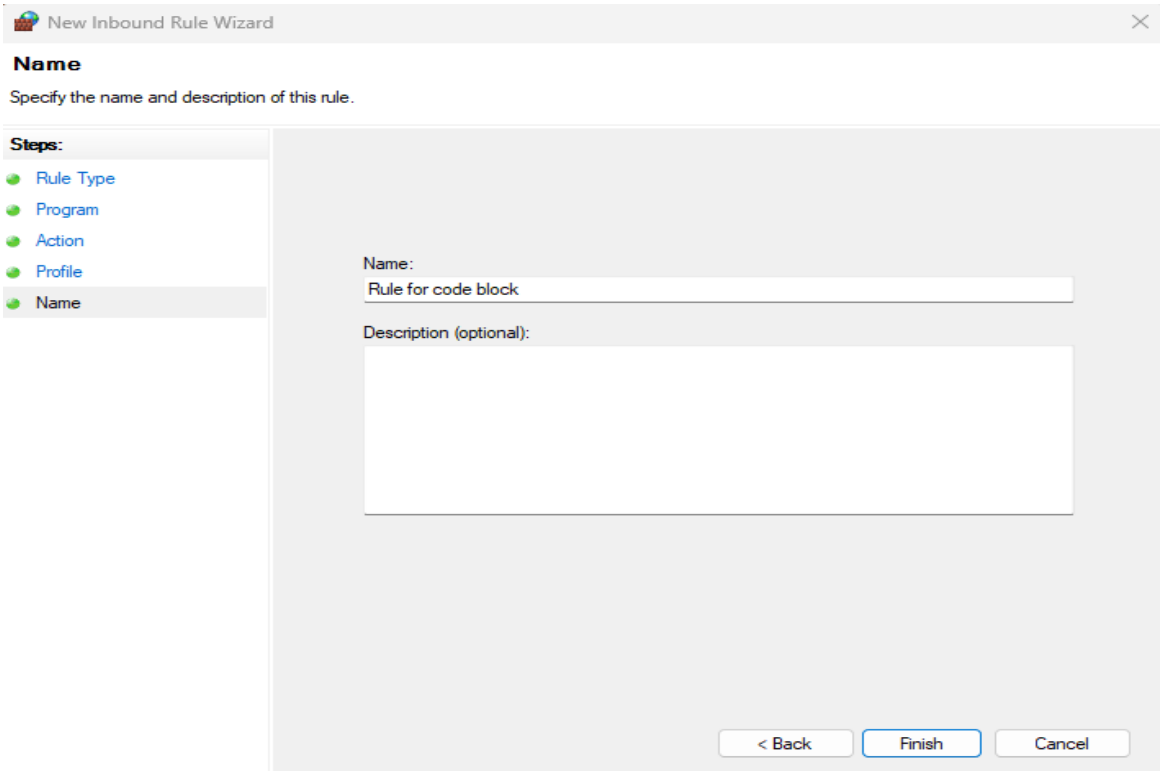


Figure 4.10 Naming of new Inbound Rules for Windows Defender Firewall

- Creating Outbound Rules:
  - In the left pane, click on Outbound Rules.
  - Follow the same steps as creating an inbound rule to define the outbound rule parameters. (Figure 4.11)

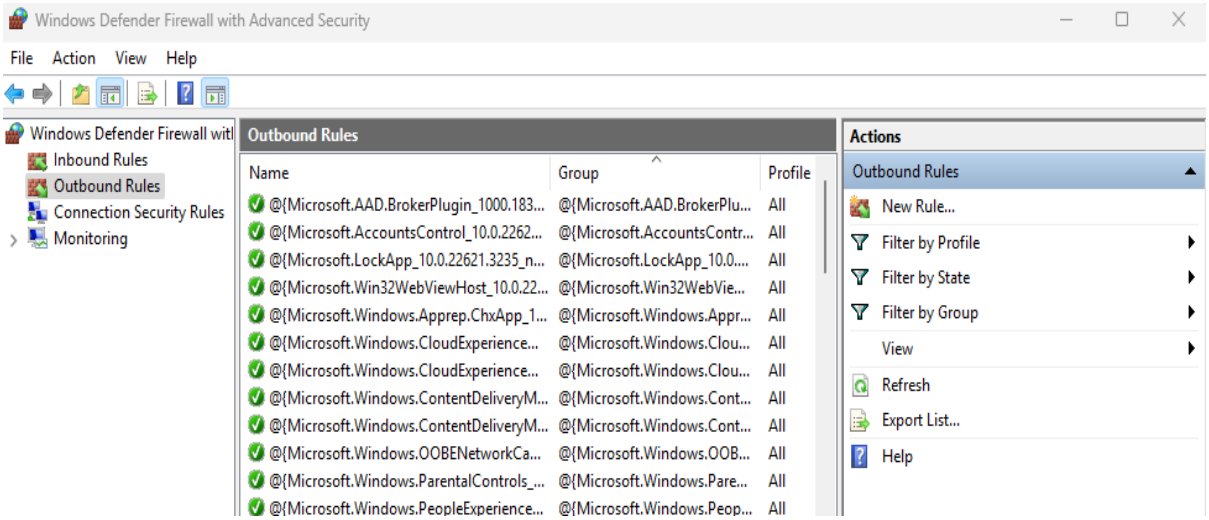


Figure 4.11 Configure new Outbound Rules for Windows Defender Firewall

- Customizing Rules:
  - To edit an existing rule, right-click on the rule and select Properties.
  - Adjust the rule settings as needed (e.g., change the action, scope, or protocol).
  - Click OK to save the changes. (Figure 4.12)

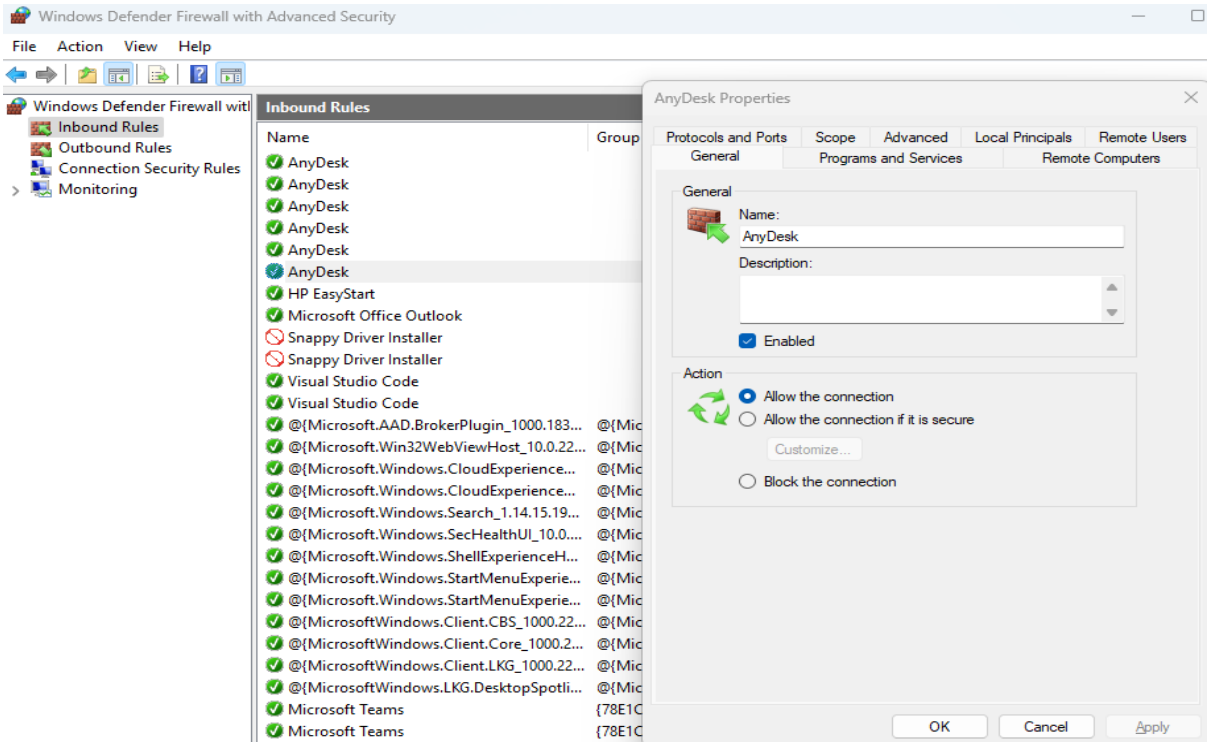


Figure 4.12 Customizing Inbound and Outbound Rules for Windows Defender Firewall

- Enabling/Disabling Firewall:
  - In the main Windows Defender Firewall window, click on Turn Windows Defender Firewall on or off. Toggle the firewall on/off for each network type. (Figure 4.13 and 4.14)

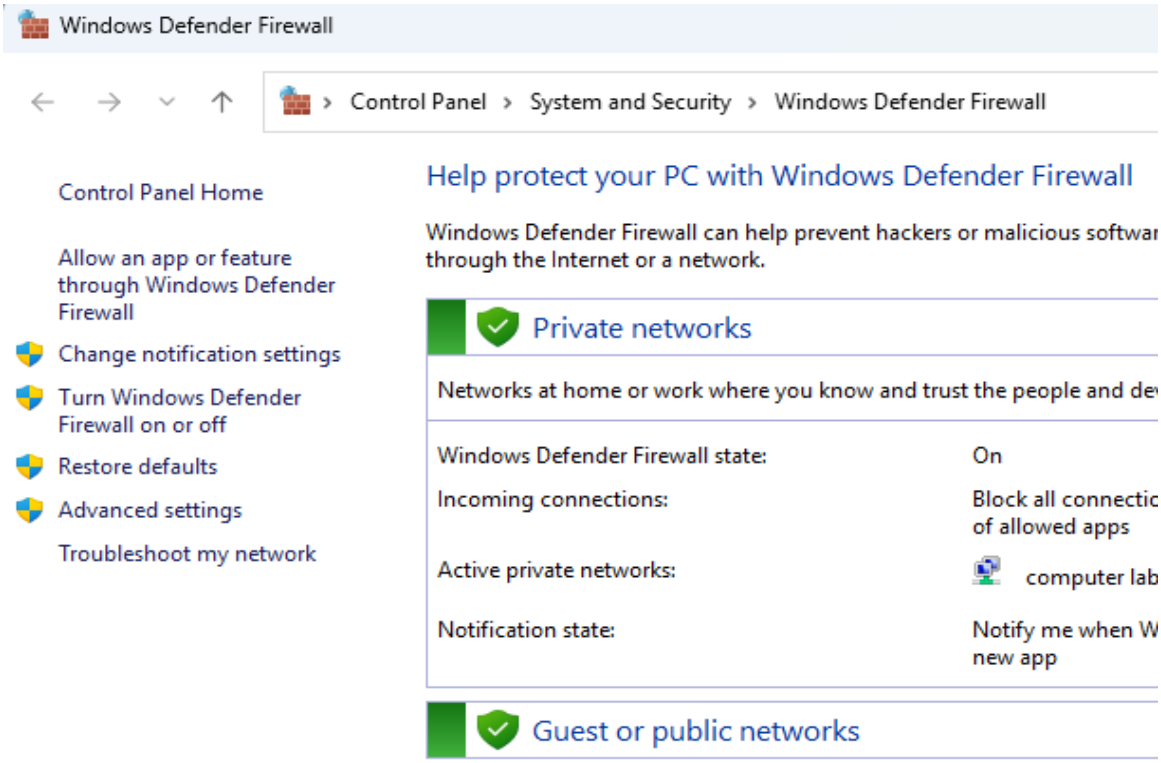


Figure 4.13 Enable-Disable Windows Defender Firewall

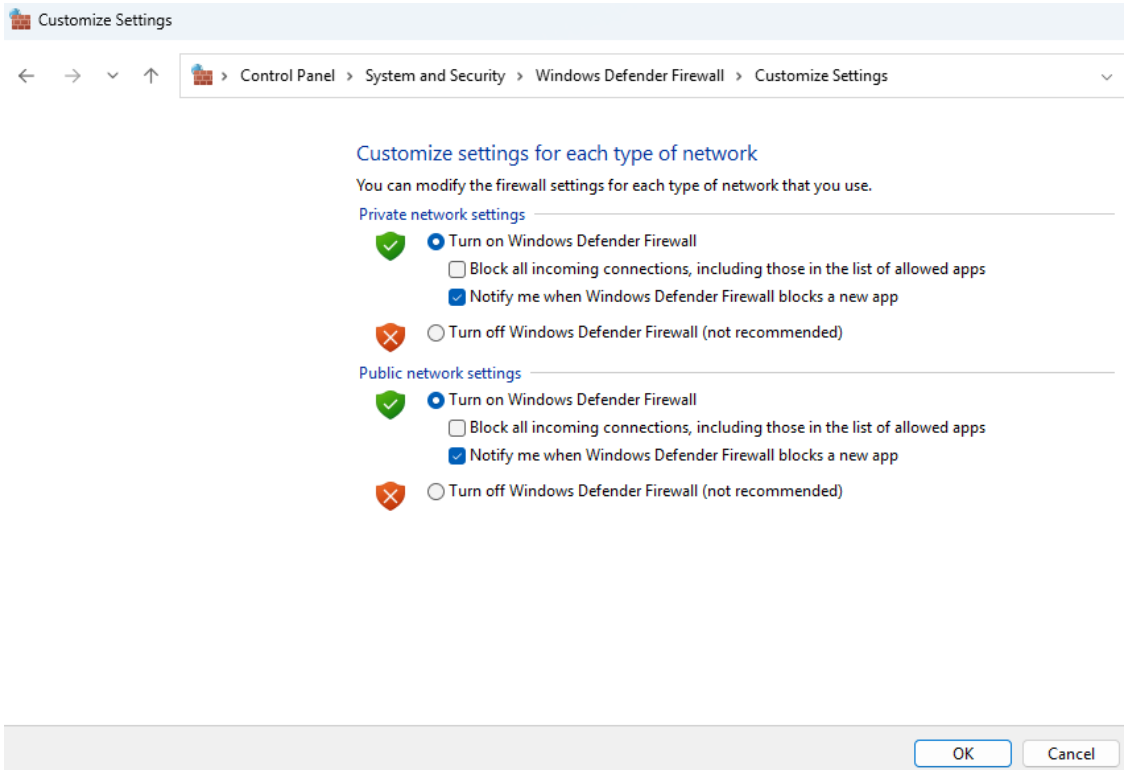


Figure 4.14 Enable-Disable Windows Defender Firewall

- Select the appropriate options to enable or disable the firewall for different network profiles (Domain, Private, Public).

By following these steps, users can configure Windows Firewall to enhance their system's security, protecting it from potential network-based threats.

4.2 Windows Defender Antivirus

Windows Defender Antivirus is a built-in antivirus program that provides real-time protection against malware, viruses, and other security threats.

Features:

- **Automatic scans:** It automatically scans all types of files like doc, image, audio and videos.
- **Real-Time Protection:** Continuously monitors the system for threats and automatically takes action to protect against malware.
- **Cloud-Based Protection:** Utilizes cloud-based machine learning to detect and respond to new threats quickly.
- **Automatic and Regular updates via Windows Update:** Regularly updates virus definitions to stay current with emerging threats.

Example: If any user downloads a suspicious file, Windows Defender Antivirus will scan the file for malware and quarantine it if detected, preventing potential damage to the system.

Steps to access and use Windows Defender Antivirus

1. Open the Windows Security app. (*Figure 4.15)*

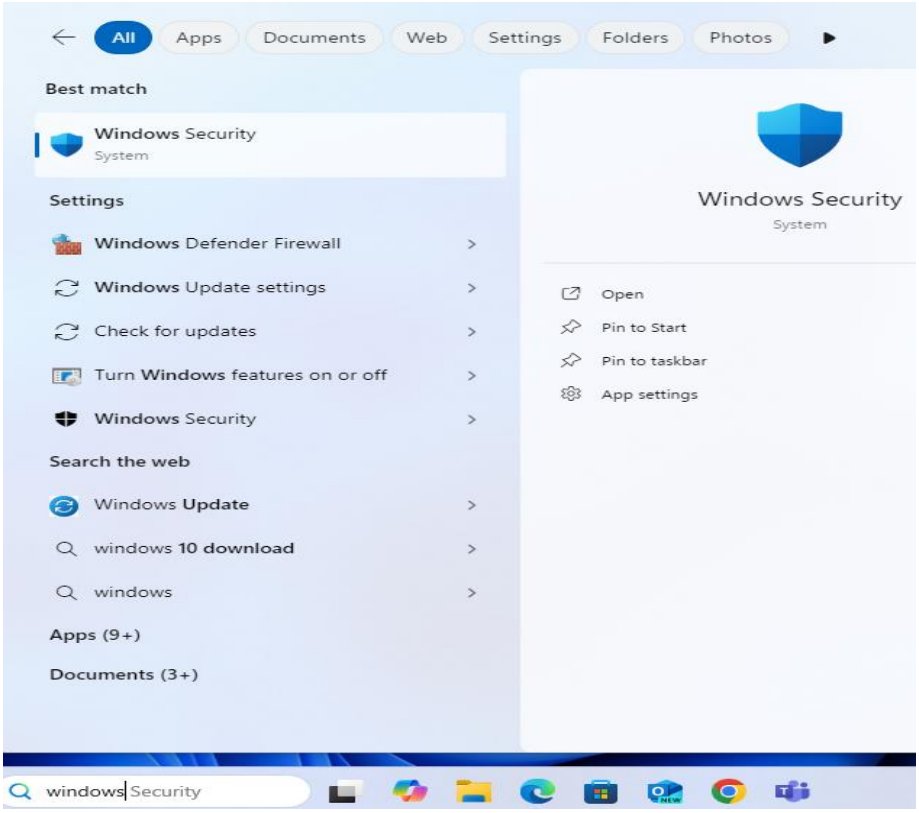


Figure 4.15 Windows Security App

2. Click Virus & threat protection. (*Figure 4.16)*

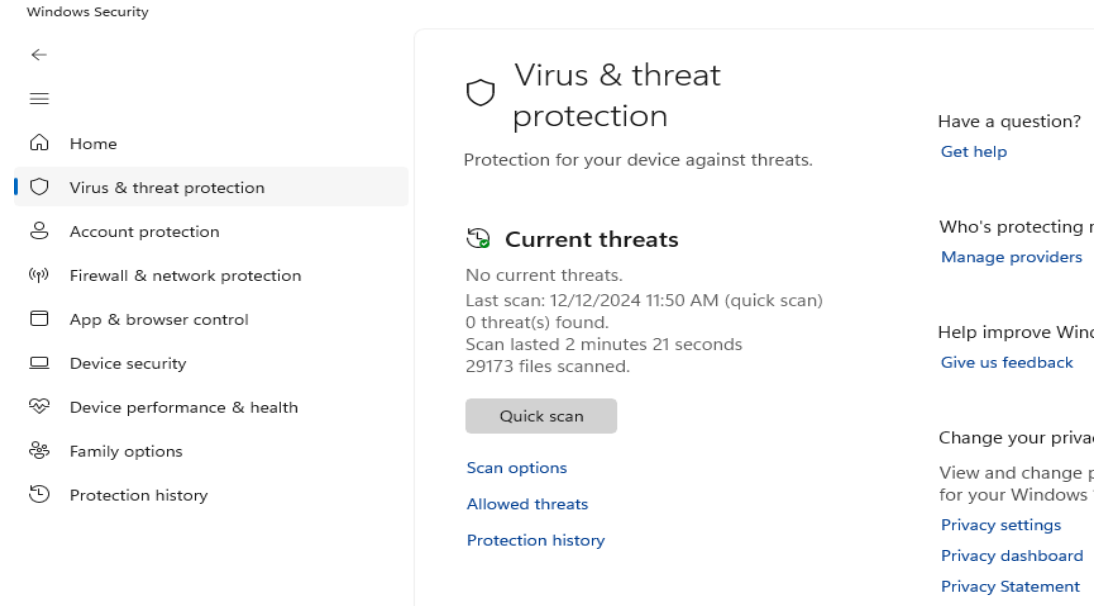


Figure 4.16 Virus & Threat Protection in Windows Security App

3. Run a quick scan or full system scan.(*Figure 4.17)*

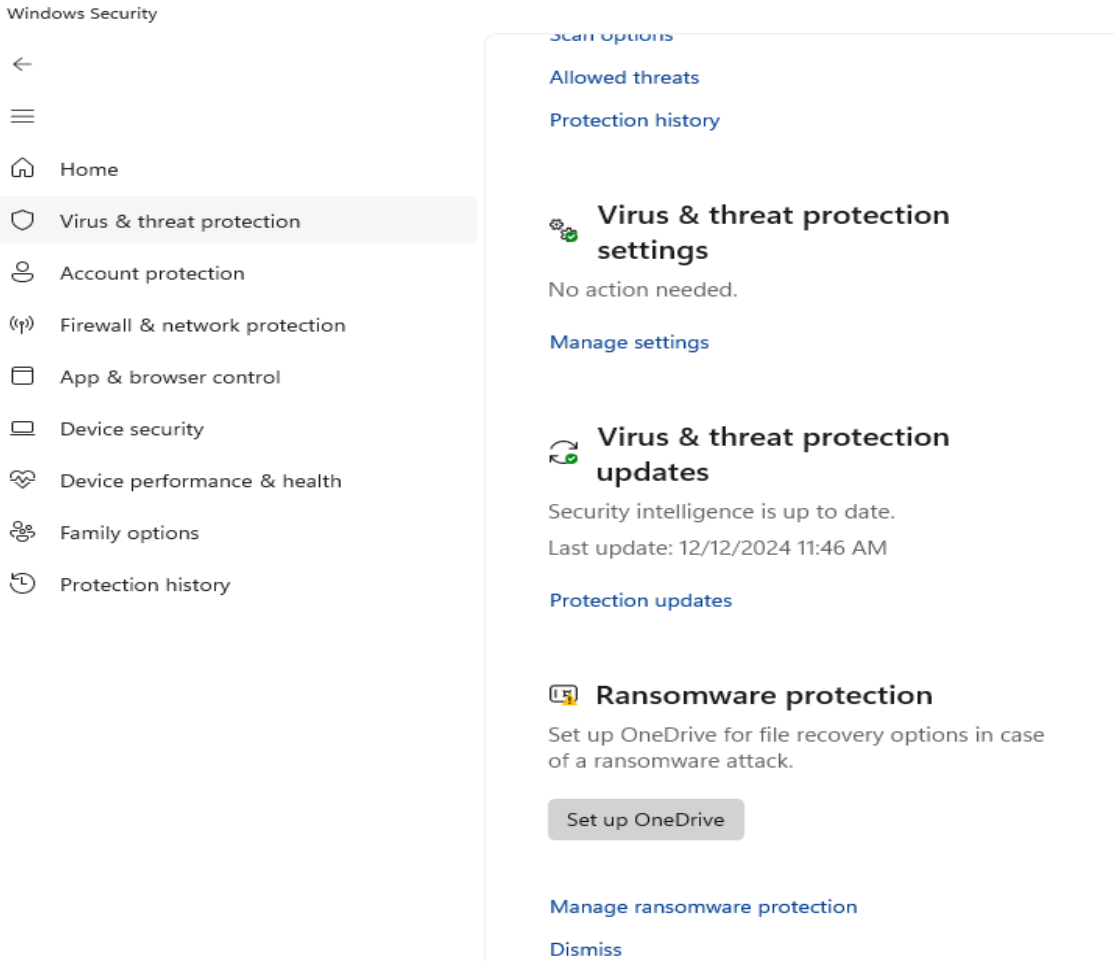


Figure 4.17 Quick Scan of Virus & Threat Protection in Windows Security App

4. Review the threat history and take action on quarantined files.

4.3 BitLocker

BitLocker is a windows OS based security tool which secures sensitive data by encrypting entire drives of the computer system. It is a full-disk encryption feature that protects data by encrypting the entire drive. It restricts unauthorized access to the data in it, even if the hard disk is lost or stolen.

Key Features:

- It encrypts the entire drive to protect data from unauthorized access.
- It requires USB key for authentication
- It uses Trusted Platform Module (TPM) for improving security by storing encryption keys in hardware.
- It provides recovery keys to unlock the drive if the user forgets the password or loses access.

Example: If a windows OS based laptop with BitLocker enabled is stolen, the thief or attacker cannot access the data on the drive without the encryption key, ensuring that sensitive information remains protected.

Steps to access and use BitLocker:

1. Search for BitLocker in the Start Menu and select Manage BitLocker. (*Figure 4.18)*

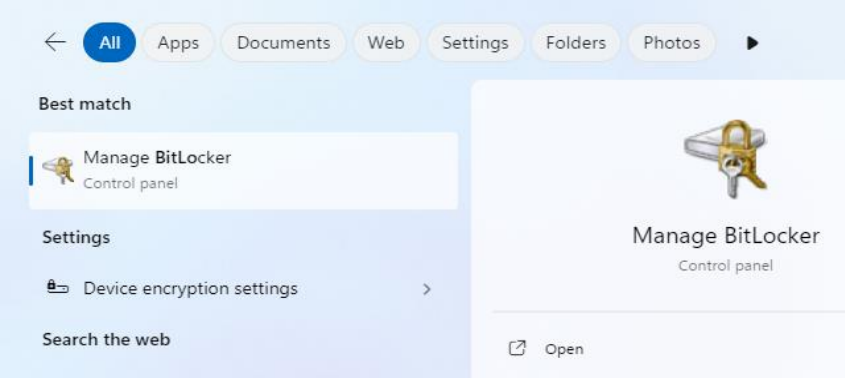


Figure 4.18 Accessing Manage Bitlocker through Control Panel

2. Choose the drive to encrypt. (*Figure 4.19)*
3. Set a password or insert a USB key for access

Figure 4.19 Turn on Bitlocker Drive Encryption for a selected drive

4. Backup recovery key (*Figure 4.20)*

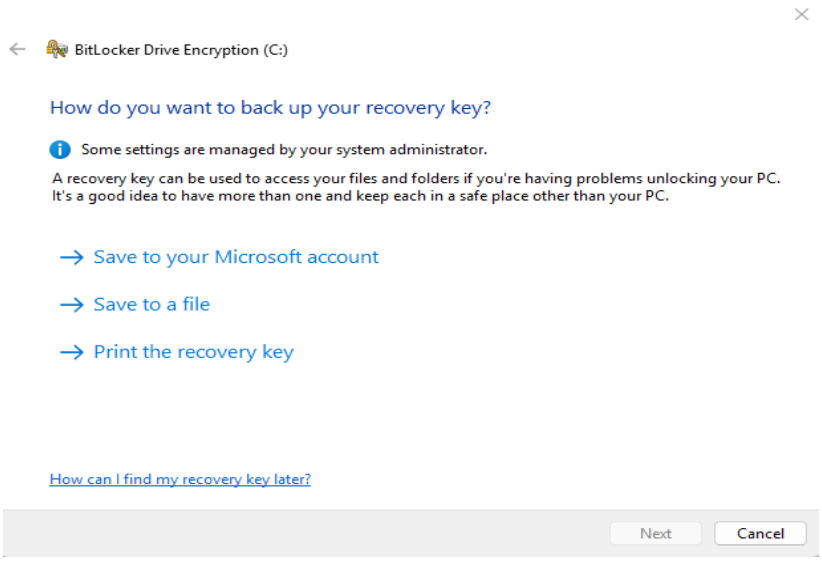


Figure 4.20 Making Backup of Bitlocker Recovery Key

5. Save the recovery key securely. (*Figure 4.21)*

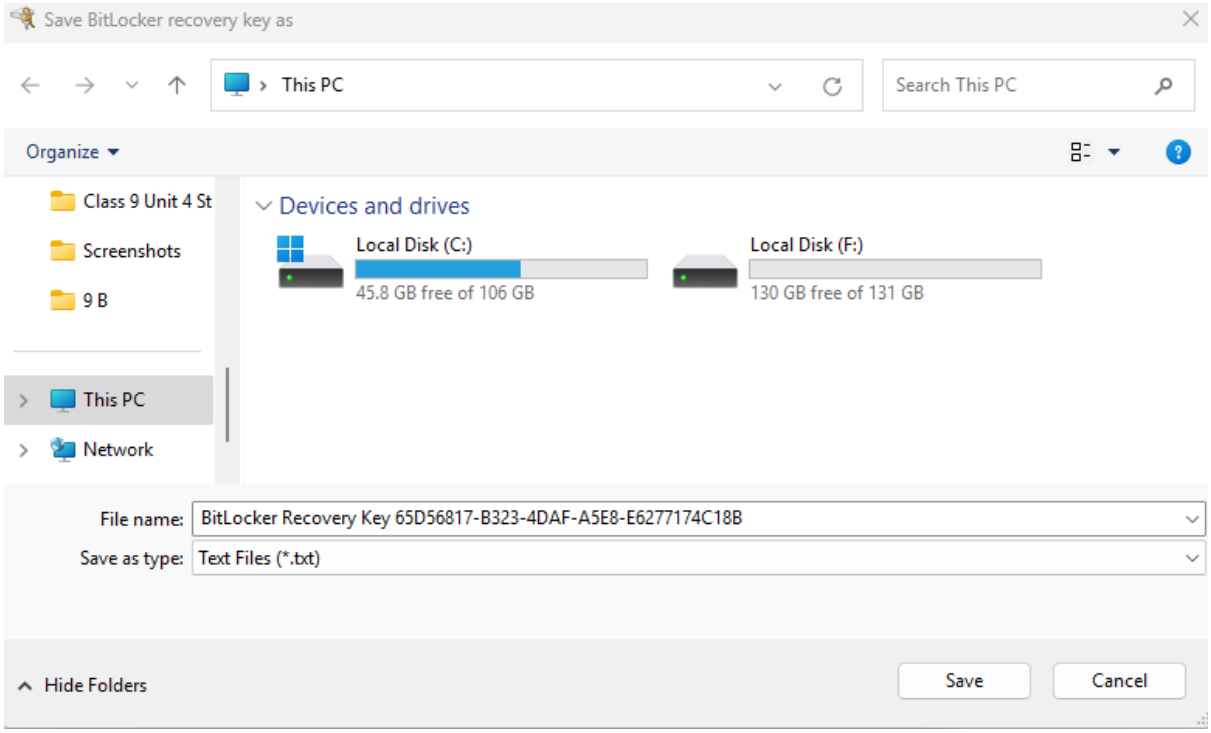


Figure 4.21 Saving Bitlocker Recovery Key

Points to Remember:

Security Tools For Windows OS:

- Windows Defender Antivirus
- Windows Firewall
- BitLocker
- User Account Control

Windows Defender Antivirus provides real-time protection against malware and viruses. It performs automatic scans and threat management.

Windows Firewall monitors and controls network traffic (inbound and outbound). Its advanced settings allow custom rule creation.

BitLocker encrypts entire drives to secure sensitive data. It protects data even if the device is lost or stolen. It requires a TPM or USB key for encryption authentication.

User Account Control (UAC)

UAC prevents unauthorized changes to the OS by prompting for administrative credentials when critical actions are performed.

Practical Activity 4.1

Objective: Learners will configure windows firewall of Windows Operating System

Tools & Platform Needed: Desktop/Laptop having Windows Operating System

Group Formation and Task Assignment:

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

Step 2. Assign each group configuration tasks like new inbound and outbound rules, update existing inbound and outbound rules, enabling/disabling firewall

Procedure to Configure new inbound and outbound rules:

Steps: Follow the steps given above in section 3.3.2 of this chapter

Procedure to Customize existing inbound and outbound rule :

Steps: Follow the customization steps given above in section 3.3.2 of this chapter

Procedure to enabling/disabling firewall:

Steps: Follow the steps for enabling/disabling firewall given above in section 4.1.1 of this chapter

Document the process:

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

Practical Activity 4.2

Objective: Learners will configure Bitlocker encryption on selected hard disk drive of a designated Desktop/Laptop

Tools & Platform Needed: Desktop/Laptop having Windows Operating System

Procedure:

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

Step 2. Assign each group selected hard disk drive of a designated Desktop/Laptop

Steps to configure Bitlocker encryption: Follow the steps given above in section 4.3 of this chapter

Document the above steps and findings: Each group will showcase their findings in the form of presentation slides in front of class and discuss the importance of Bitlocker Encryption in Information security.

List of other suggested practical activities:

- **Virus and Threat Protection:** Explore virus and threat protection option available in Windows defender antivirus as part of Windows Security
- Encrypting a Removable Drive with BitLocker

1. Insert the Removable USB Drive into the computer
2. Turn on BitLocker:
    a. Go to the Control Panel and select BitLocker Drive Encryption.
    b. Under Removable data drives, select Turn on BitLocker for the USB drive.
3. Set Up Encryption:
    a. Choose how to unlock the drive (e.g., password).
    b. Select how to back up the recovery key.
    c. Choose the encryption mode and start encrypting the drive

Demonstration of the security tools (Antivirus tools, firewall, bitlocker etc. using (simulation/video) **List of other suggested practical activities:**

- **Virus and Threat Protection:** Explore virus and threat protection option available in Windows defender antivirus as part of Windows Security
- Encrypting a Removable Drive with BitLocker

4. Insert the Removable USB Drive into the computer
5. Turn on BitLocker:
    a. Go to the Control Panel and select BitLocker Drive Encryption.
    b. Under Removable data drives, select Turn on BitLocker for the USB drive.
6. Set Up Encryption:
    a. Choose how to unlock the drive (e.g., password).
    b. Select how to back up the recovery key.
    c. Choose the encryption mode and start encrypting the drive

- Demonstration of the security tools (Antivirus tools, firewall, bitlocker etc. using (simulation/video)

SUMMARY

Overview

- Operating system (OS) security ensures confidentiality, integrity, and availability of system resources.
- It protects against unauthorized access, data breaches, and cyber threats.

Access Control in OS Security

➔ Purpose: Restricts unauthorized access to system resources.

- ➔ Components:
  - ◆ Authentication: Verifies user identity.
  - ◆ Authorization: Defines permissions for authenticated users.
- ➔ Access Control Models:
  - ◆ Discretionary Access Control (DAC): Resource owners control permissions.
  - ◆ Mandatory Access Control (MAC): Permissions enforced by policies.
  - ◆ Role-Based Access Control (RBAC): Permissions assigned based on roles.
  - ◆ Attribute-Based Access Control (ABAC): Permissions based on user attributes.

Security Tools For Windows OS

- ➔ Windows Defender Antivirus:
  - ◆ Real-time protection against malware and viruses.
  - ◆ Features automatic scans and threat management.
- ➔ Windows Firewall:
  - ◆ Monitors and controls network traffic (inbound and outbound).
  - ◆ Advanced settings allow custom rule creation.
- ➔ BitLocker:
  - ◆ Encrypts entire drives to secure sensitive data.
  - ◆ Protects data even if the device is lost or stolen.
  - ◆ Requires TPM or USB key for encryption authentication.
- ➔ User Account Control (UAC):
  - ◆ Prevents unauthorized system changes.
  - ◆ Manage quarantined threats and review threat history.

Best Practices

- Regularly update Windows and security tools.
- Enable multi-factor authentication (MFA) for added security.
- Backup data to prevent loss in case of a cyberattack.
- Use Group Policy for organization-wide security enforcement.

Conclusion

By implementing robust access control and leveraging built-in Windows security tools like Firewall, Defender Antivirus, and BitLocker, the operating system can serve as a strong defense against cyber threats.

ASSESSMENT

A. Multiple Choice Questions

1. What is the primary function of Windows Defender Antivirus?
   (a) Monitor network traffic
   (b) Encrypt files and folders

(c) Provide real-time protection against malware
(d) Manage user accounts

2. What is the purpose of BitLocker in Windows OS?
(a) Manage software updates
(b) Encrypt the entire drive
(c) Block unwanted websites
(d) Monitor system performance

3. Which security tool uses Trusted Platform Module (TPM) for enhanced security?
(a) Windows Defender Antivirus
(b) Windows Firewall
(c) BitLocker
(d) Digital Certificates

4. How does Windows Firewall primarily enhance system security?
(a) By encrypting all incoming data
(b) By blocking unauthorized network traffic
(c) By scanning files for viruses
(d) By managing user permissions

5. Which term describes converting plaintext into ciphertext?
(a) Decryption
(b) Hashing
(c) Encoding
(d) Encryption

6. What does VPN stand for in the context of network security?
(a) Virtual Personal Network
(b) Verified Public Network
(c) Virtual Private Network
(d) Virtual Protected Network

7. What is the primary objective of access control in OS security?
(a) Speed up processing
(b) Prevent unauthorized access
(c) Increase network traffic
(d) Reduce system logs

8. What feature in Windows prevents unauthorized changes to the operating system?
(a) Firewall
(b) BitLocker
(c) User Account Control (UAC)
(d) Windows Defender

9. Which Windows tool is used for full-disk encryption?
   (a) Firewall
   (b) BitLocker
   (c) Windows Defender
   (d) Event Viewer

10. Where can you configure advanced rules for Windows Firewall?
   (a) Virus & threat protection
   (b) Advanced settings in Firewall
   (c) Control Panel > Power Options
   (d) Device Manager

11. What is a key advantage of Windows Defender Antivirus?
   (a) Requires third-party software updates
   (b) Provides real-time protection
   (c) Only detects spyware
   (d) Replaces the need for a firewall

12. How can you run a full system scan in Windows Defender?
   (a) Control Panel > System Settings
   (b) Windows Security > Virus & threat protection
   (c) Device Manager > Update Drivers
   (d) Firewall & network protection > Scan Options

B. Fill in the blanks:

1. The process of converting ciphertext back into plaintext is known as _____.
2. _____ encryption uses a pair of keys, one public and one private.
3. Windows Defender Antivirus offers _____ protection against malware.
4. BitLocker uses _____ to store encryption keys securely in hardware.
5. The _____ model assigns access permissions based on user attributes.
6. In a network security context, VPN stands for _____.
7. _____ is a built-in Windows security tool that monitors and controls network traffic.
8. A firewall monitors and controls _____ and _____ traffic.
9. The most granular control in Windows Firewall can be configured under _____.
10. The Windows tool for managing network security is called _____.

C. True or False

1. Windows Firewall can only block incoming network traffic.
2. Role-Based Access Control assigns permissions based on individual user discretion.
3. BitLocker is used to encrypt individual files and folders, not the entire drive.

4. Hash functions convert data into a fixed-size string to ensure data integrity.
5. VPNs create secure connections by encrypting data over the internet.
6. Mandatory Access Control allows users to set their own access permissions.
7. Windows Defender Antivirus requires a separate subscription to use.
8. Discretionary Access Control is based on a central authority setting access policies.
9. Windows Defender Antivirus can quarantine malicious files.
10. A strong password is unnecessary when BitLocker is enabled.

D. Short Answer type questions.

1. Explain the primary function of Windows Defender Antivirus.
2. How does BitLocker enhance the security of a Windows OS device?
3. What is the role of a VPN in network security?
4. How can you configure advanced rules in Windows Firewall?

E. Long Answer type questions.

1. Explain the different types of inbound and outbound rules of Windows Firewall.
2. Describe the features of Windows Firewall, Windows Defender Antivirus, and BitLocker, and explain how they contribute to securing a Windows operating system.
3. Explain the step-by-step process of configuring Windows Firewall settings by creating inbound and outbound rules and creating a custom rule to manage network traffic.

ANSWER KEY

A. Multiple Choice Questions

1.c, 2.b, 3.c, 4.b, 5.d, 6.c, 7.b, 8.c, 9.b, 10.b, 11.b, 12.b

B. Fill in the Blanks

1. 1.Decryption, 2.Asymmetric-key, 3.real-time, 4.TPM, 5.Attribute-Based Access Control (ABAC), 6.Virtual Private Network, 7.Windows Firewall, 8.incoming and outgoing, 9.Advanced settings, 10.Windows Firewall

C. True or False

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

Chapter-5

Wireless Networks and Security

Heena was working on her laptop at a local coffee shop, connected to the free Wi-Fi. She didn't think twice—until she noticed a strange pop-up from her bank. A large, unauthorized transaction was being processed. Panicked, Heena tried to log into her account, but it was too late. A hacker had stolen her credentials.

Heena called her brother, Jitesh, who worked in cybersecurity. He quickly explained that she'd fallen victim to a "man-in-the-middle" attack. By setting up a fake Wi-Fi network, the hacker had intercepted Heena's data, including her banking info.

"Public Wi-Fi networks are risky," Jitesh said. "Hackers can snoop on unencrypted connections, stealing sensitive information."

He helped Heena secure her accounts and gave her some crucial cyber safety tips. Always avoid using public Wi-Fi for sensitive transactions, use a VPN, and double-check Wi-Fi network names. Jitesh also recommended enabling two-factor authentication on her accounts.

Heena learned her lesson the hard way but was now much more cautious online. She promised to share these tips with friends to help them stay safe.

This chapter explores the fundamentals of wireless networks, their types, and the key aspects of wireless security, including common threats and best practices.

5.1 Introduction to Wireless Networks

Wireless networks enable devices to connect and communicate without physical cables, relying on radio frequency (RF) signals to transmit data.

Characteristics of Wireless Networks

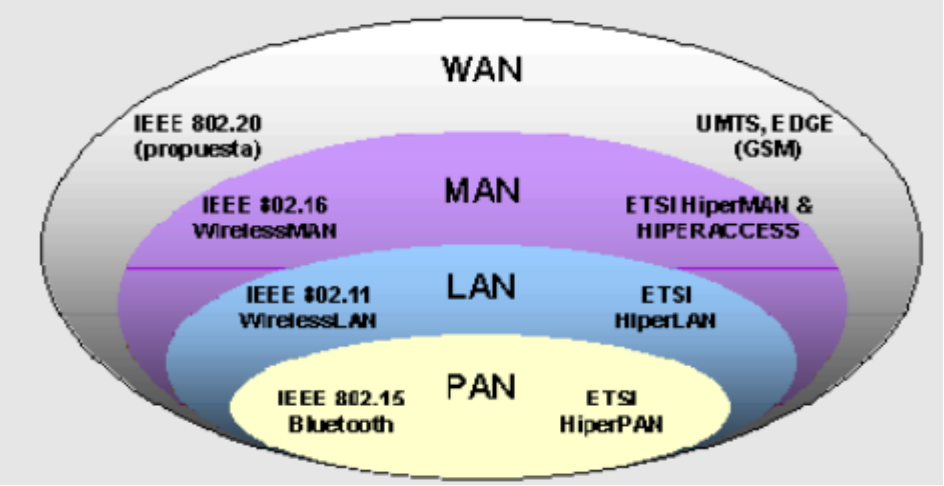
- A wireless network uses radio waves to connect devices such as laptops, smartphones, and tablets to the internet and other networks without the need for physical cables.

- Wireless networks provide the freedom to access network resources from almost anywhere within the network's coverage area.
- Wireless networks have revolutionized the way we connect and communicate, providing mobility, convenience, and flexibility. Users can access resources from anywhere within the network's range.
- Wireless networks are scalable. It is easy to add devices without additional cabling.
- Wireless networks are cost-effective compared to wired networks.

Challenges For Wireless Networks

- Wireless networks may face signal interference issues due to disruptions from other RF sources.
- Wireless networks may have limited range. Its coverage depends on the power and type of access point.
- Wireless networks, due to their open medium, are inherently less secure than wired networks. Effective security measures are required to protect data, ensure user privacy, and prevent unauthorized access.

5.1.1 Types of Wireless Networks



1. **Wireless Personal Area Network (WPAN):** It is a very short-range network which connects devices within a short range, typically within a few meters.

   Example: Bluetooth and Zigbee are examples of technology which are based on WPAN standard. They provide connections between smartphones, headphones, and smartwatches.

2. **Wireless Local Area Network (WLAN):** It connects devices within a limited area, such as a home, office, or campus.

   Example: Wi-Fi networks used in homes and businesses. Most commonly implemented as Wi-Fi (IEEE 802.11 standards)

3. **Wireless Metropolitan Area Network (WMAN):** It covers a larger area than WLANs, such as a city, rural areas or town.

   Example: WiMAX networks that provide broadband access to urban areas.

4. **Wireless Wide Area Network (WWAN):** It covers a broad area, such as a country or continent, using internet and cellular technology.

   Example: 4G and 5G cellular networks used by mobile carriers.

5.1.2 Major components of Wireless Networks

1. **Access Points (APs):** Access points are devices that connect wireless clients to the wired network and manage wireless connections. An access point (AP) is a network device that bridges wired and wireless networks. Consumer APs are often called "wireless routers" because they typically also serve as both internet routers and firewalls.

   Example: Wi-Fi routers in homes and offices. See Figure 5.1, it is an access point manufactured by Cisco for small businesses.

Figure 5.1 Cisco Small Business 500 Series Access Point-Wireless Router

2. **Wireless Clients:** Devices that connect to the wireless network, such as Desktops, laptops, smartphones, and tablets.

   Example: A laptop connecting to a home Wi-Fi network.

3. **Network Interface Cards (NICs):** Hardware components in wireless clients that enable wireless communication.

   Example: Wi-Fi adapters in Desktops, laptops and smartphones.

Figure 5.2 (a) ZEBRONICS Wi-Fi adapter Desktop

Figure 5.2 (b) tp-link Wi-fi NIC card for

4. **Wireless Controllers:** Centralized devices that manage multiple access points and wireless network settings.

   Example: Controllers used in large enterprise networks to manage Wi-Fi access points. See in Figure 5.3, a Cisco wireless controller of catalyst series 9800-L is capable of controlling 250-500 access points, 5000-10000 wireless clients, andsupports maximum 4096 WLANs with 5 to 10 Gbps throughput.

Figure 5.3 Cisco Catalyst 9800-L Wireless Controller

Table 5.1 A concise overview of the different 802.11 WLAN types

802.11 Standard	Frequency	Data Rate	Range	Key Features
802.11a (1999)	5 GHz	Up to 54 Mbps	Lower than 802.11b/g due to higher frequency	Less interference, suitable for densely populated areas
802.11b (1999)	2.4 GHz	Up to 11 Mbps	Better than 802.11a	First widely adopted standard, significant interference from other devices
802.11g (2003)	2.4 GHz	Up to 54 Mbps	Similar to 802.11b	Combines the best of 802.11a and 802.11b, backward compatible with 802.11b
802.11n (Wi-Fi 4) (2009)	2.4 GHz, 5 GHz	Up to 600 Mbps	Improved over previous standards	Introduced MIMO technology for better performance
802.11ad (WiGig) (2012)	60 GHz	Up to 7 Gbps	Very short, typically within a room	High-speed data transfer over short distances

802.11ac (Wi-Fi 5) (2014)	5 GHz	Up to 3.46 Gbps (theoretical)	Better than 802.11n due to beamforming	Significant improvements in speed and capacity, supports more devices
802.11ah (HaLow) (2017)	Sub-1 GHz	Up to 347 Mbps	Extended range compared to 2.4 GHz and 5 GHz	Suitable for IoT applications due to better range and lower power consumption
802.11ax (Wi-Fi 6) (Wi-Fi 6E) (2019)	2.4 GHz, 5 GHz, potentially 6 GHz	Up to 9.6 Gbps (theoretical)	Improved over 802.11ac	Enhanced performance in dense environments, improved battery life
802.11be (Wi-Fi 7) (2024)	2.4/5/6 GHz	Up to 46 Gbps	Improved over 802.11ax	Ultra-high throughput

Points to Remember:

Wireless Networks provide mobility, scalability, and cost effective systems.

Wireless networks use radio frequency (RF) signals or waves to connect the devices for communication, eliminating the need for physical cables.

Wireless networks face issues like security, signal interference, limited range, and security vulnerabilities. Wireless networks are more vulnerable due to their open medium.

Wireless Network Types:

- WLAN (Wireless Local Area Network): Wi-Fi
- WMAN (Wireless Metropolitan Area Network): WiMAX
- WWAN (Wireless Wide Area Network): cellular networks like 4G and 5G, IoT devices
- WPAN (Wireless Personal Area Network): Bluetooth, Zigbee

Wireless Networks components:

- Access Points (APs)
- Wireless clients
- Network Interface Cards (NICs) and wireless adapters

Wireless controllers

5.2 Wireless Security

Wireless networks are susceptible to various security threats, making it essential to implement robust security measures. Wireless security aims to protect the network from unauthorized access, data breaches, and other cyber threats.

Wireless networks offer convenience and flexibility, but they also present unique security challenges. Understanding the fundamentals of wireless networks and implementing robust security measures can protect against various threats. By following best practices and staying informed about the latest security protocols, users can ensure the safety and reliability of their wireless networks. Wireless networks are indispensable to modern life, enabling unprecedented connectivity and mobility.

However, their open nature necessitates robust security measures to safeguard data and ensure reliable communication. As technology evolves, adopting advanced security protocols and best practices will be essential to mitigating emerging threats.

5.2.1 Wireless Security Goals

- **Confidentiality:** To ensure data is accessible only to authorized users.
- **Integrity:** To protect data from unauthorized modification.
- **Authentication:** To verify user identities before granting access.
- **Availability:** To ensure the network is operational and accessible to legitimate users.

5.2.2 Major Security Risks and Threats across Wireless Networks

1. **Eavesdropping:** Attackers intercept data transmitted over wireless networks, listen to wireless communications and threaten the confidentiality of sensitive information.

   Example: An attacker capturing unencrypted data transmitted over a public Wi-Fi network.

2. **Unauthorized Access:** Attackers exploit weak passwords or open networks to gain entry. It can lead to misuse of resources and data breaches. Intruders gain access to the wireless network without permission.

   Example: A neighbor connecting to your home Wi-Fi network without your knowledge.

3. **Man-in-the-Middle (MITM) Attacks:** Interception and manipulation of communications between devices.

4. **Denial of Service (DoS) Attacks:** Attackers flood the network with excessive traffic to disrupt and deny services to its legitimate users.

   Example: An attacker using a flood of requests to overwhelm a Wi-Fi network, making it unusable.

5. **Phishing Access Points:** Attackers use unauthorized devices to set up fake access points mimicking legitimate access points to steal data.

   Example: An attacker setting up a fake Wi-Fi hotspot in a coffee shop to capture user credentials.

5.2.3 Existing Wireless Security Protocols and Encryption Techniques

1. **WEP (Wired Equivalent Privacy):** An older encryption and security protocol with known vulnerabilities.

Usage: It is rarely used today due to its weak encryption and vulnerable to attacks.

2. **WPA (Wi-Fi Protected Access):**

   WPA is an improved security protocol that replaced WEP.

   Usage: It provides better encryption and security than WEP but has been largely superseded by WPA2.

3. **WPA2 (Wi-Fi Protected Access II):** A widely used security protocol that offers strong encryption and authentication.

   Usage: It is commonly used in home and business Wi-Fi networks.

4. **WPA3 (Wi-Fi Protected Access III):** The latest security protocol that provides enhanced protection against brute-force attacks and better encryption.

   Usage: It is increasingly adopted in modern wireless devices for improved security.

5. **Virtual Private Networks (VPNs):** It creates secure, encrypted tunnels for data transmission over wireless networks.

5.2.4 Authentication Mechanisms in Wireless Networks

1. **MAC Address Filtering:** It restricts network access to approved devices.
2. **Pre-shared Key (PSK):** Users must know a shared password to connect to the network.
3. **802.1X Authentication:** It is an enterprise-grade solution using RADIUS servers for secure user authentication.

5.2.5 Tips for ensuring security of Wireless Networks

1. **Use Strong Encryption Protocol:** Use WPA3 encryption for the highest level of security. If WPA3 is not available, use WPA2. Configure your Wi-Fi router to use WPA2 or WPA3 encryption.
2. **Change Default Settings:** Change default SSID (network name) and administrative passwords to prevent unauthorized access. Set a unique network name and strong password for your Wi-Fi router.
3. **Enable Firewalls:** One should enable all types of firewalls on Wi-Fi routers which protects devices and networks from unauthorized access. Also configure the firewall settings on the router for better network security.
4. **Disable Unused Features:** Disable WPS to prevent vulnerabilities that can be exploited by attackers. Turn off the WPS(Wi-Fi Protected Setup) feature in Wi-Fi router settings.
5. **Enable Network Authentication with strong passwords:** Use strong, unique passwords for network access and change them regularly. Set a complex password for your Wi-Fi network and update it periodically.
6. **Regularly Monitor Network Activity:** Regularly check for unauthorized devices connected to your network. Use network monitoring tools to detect anomalies and remove unauthorized access.

7. **Update Firmware and other important softwares:** Keep your Wi-Fi router firmware updated to patch security vulnerabilities. Regularly check for and install firmware updates for your Wi-Fi router.

Points to Remember:

Wireless Security Threats and Risks

- Unauthorized Access
- Eavesdropping
- Man-in-the-Middle (MitM) Attacks
- Denial of Service (DoS) Attacks
- Phishing access points

Wireless Security Protocols

- WEP: An older, less secure protocol.
- WPA: Improved security over WEP.
- WPA2: Widely used, strong encryption and authentication.
- WPA3: Latest, enhanced protection against brute-force attacks.

Authentication Mechanisms: MAC address filtering, pre-shared keys, and 802.1X authentication.

Actions to be taken for ensuring Wireless Security:

- use strong passwords, Change default SSID and passwords
- use strong encryption (WPA2 or WPA3)
- enable firewalls
- update firmware
- disable unused features

Disable unnecessary updates like WPS and monitor network activity

Practical Activity 4.1.

Objective: Objective: To set up a Wi-Fi network and learn basic security measures.

Tools and Platform Needed: Wireless router, Desktop, laptop/smartphone, internet connection.

Procedure:

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

Step 2. Instructor will demonstrate a sample SSID, Passwords, encryption protocol adopted

Step 3. Instructor will Configure a wireless router by accessing the router's admin panel and Set a unique SSID (network name).

Step 4. Instructor will enable WPA2 (or WPA3 if WPA3 is available)

Step 5. Instructor will disable unused features like WPS.

Step 6. Instructor will configure the firewall settings on the router to block unauthorized access.

Step 7. Instructor will test the connection by connecting a device to established Wi-Fi Network.

Step 8. All group members will explore and document above activity.

Step 9. The member of each group will perform above steps and each group will set up a wireless network & discuss the security of a wireless network could be enhanced using encryption and other security measures..

Practical Activity 4.2.

Objective: To detect and mitigate the presence of Phishing Wi-fi access points within a network environment.

Tools and Platform Needed: Wi-Fi enabled Desktop, laptop/smartphone, internet connection, Wi-fi scanner tool

Procedure:

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

Step 2. Learner will install a Wi-Fi scanner tool such as inSSIDer, NetSpot

Step 3. Learner will scan the wireless networks using Wi-Fi scanner to identify all access points in the nearby surrounding

Step 4. Learner will analyze the above scan result to identify any SSID which look as unauthorized or unfamiliar access points

Step 5. Learners will make reports about the characteristics of each detected access point, such as SSID, MAC address, signal strength, and security encryption protocol.

Step 6. Learner will compare the detected suspected access points against the list of authorized access points available in your nearby surrounding.

Step 7. Learning will investigate and analyze further to determine the source of identified phishing access points and take appropriate action to remove or disable them.

Step 8. All group members will pendown and document above activity.

List of other suggested practical activities:

- Explore various access points (Wireless Routers) from different vendors and understand its designs and configuration which are available in Labs and institute and prepare a report.
- **Understanding IP Addressing in Wireless networks:** Learn about IP addressing and subnetting in

  wireless networks.

  Activities:

  a. Identify the IP address, subnet mask, and gateway on connected devices.
  b. Assign static IP addresses to devices.

  Tools: Command Prompt/Terminal, Router settings.
- **Packet Sniffing in Wireless Networks for understanding how data travels in wireless networks:**

  Activities:

  a. Use tools like Wireshark.
  b. Observe wireless traffic.

  Tools: Wireshark, Laptop.

SUMMARY

- Introduction to Wireless Networks:
  - Wireless networks provide mobility, scalability, and cost effective systems.
  - Wireless networks use radio frequency (RF) signals or waves to connect the devices for communication, eliminating the need for physical cables.
  - Ensuring the security of these networks is crucial.
  - Major challenges to wireless networks are Signal interference, limited range, and security vulnerabilities. Wireless networks are more vulnerable due to their open medium.
- Types of Wireless Networks:
    - WLAN (Wireless Local Area Network): Covers small areas like homes and offices. (e.g., Wi-Fi)
    - WMAN (Wireless Metropolitan Area Network): Covers larger areas like cities.
    - WWAN (Wireless Wide Area Network): Covers broad areas using cellular technology. (e.g., cellular networks like 4G and 5G).
    - WPAN (Wireless Personal Area Network): Connects devices within a short range (e.g., Bluetooth, Zigbee).
- Major components in Wireless Networks:
  - Access Points (APs): Connect wireless clients to wired networks.
  - Wireless Clients: Devices like laptops, smartphones, and tablets.
  - Network Interface Cards (NICs): Enable wireless communication in devices.
  - Wireless Controllers: Manage multiple access points and network settings.
- Wireless Security Threats and Risks:
  - Unauthorized Access: Intruders gain access without permission.
  - Eavesdropping: Interception of wireless communications.
  - Man-in-the-Middle (MitM) Attacks: Interception and alteration of communications.
  - Denial of Service (DoS) Attacks: Flooding the network with traffic.
  - Phishing access points
- Wireless Security Protocols:
  - WEP: An older, less secure protocol.
  - WPA: Improved security over WEP.
  - WPA2: Widely used, strong encryption and authentication.
  - WPA3: Latest, enhanced protection against brute-force attacks.

➔ Authentication Mechanisms:

- MAC address filtering, pre-shared keys, and 802.1X authentication.

➔ Actions to be taken for ensuring Wireless Security:

- Use strong passwords, Change default SSID and passwords, Use strong encryption (WPA2 or WPA3), enable firewalls, update firmware, disable unused features, Disable unnecessary updates like WPS and monitor network activity.

ASSESSMENT

A. Multiple Choice Questions

1. Which type of wireless network covers a small area such as a home or office?
   a) WLAN
   b) WMAN
   c) WWAN
   d) WPAN

2. Which security protocol provides the strongest encryption for Wi-Fi networks?
   a) WEP
   b) WPA
   c) WPA2
   d) WPA3

3. What does WPA stand for in wireless security?
   a) Wireless Protection Algorithm
   b) Wi-Fi Protected Access
   c) Wireless Password Authentication
   d) Wi-Fi Password Algorithm

4. What is a common practice to improve wireless network security?
   a) Use default SSID
   b) Disable encryption
   c) Change default passwords
   d) Enable WPS

5. What does VPN stand for?
   a) Virtual Personal Network
   b) Verified Public Network
   c) Virtual Private Network
   d) Virtual Protected Network

6. What type of wireless network connects devices within a short range, typically within a few meters?
   a) WLAN
   b) WMAN
   c) WWAN
   d) WPAN

7. Which of the following is a characteristic of a Wireless Personal Area Network (WPAN)?
   a) Covers large geographic areas
   b) Uses Bluetooth or Zigbee technology
   c) Relies on RADIUS authentication
   d) Provides internet via satellite

8. What is the primary standard used for Wireless Local Area Networks (WLANs)?
   a) IEEE 802.3
   b) IEEE 802.15
   c) IEEE 802.11
   d) IEEE 802.16

9. What does WPA3 offer that WPA2 does not?
   a) Basic encryption
   b) Advanced key management and security protocols
   c) Physical device connectivity
   d) Open network functionality

10. What is the main purpose of a Virtual Private Network (VPN) in wireless networks?
   a) Enhancing speed
   b) Creating secure, encrypted tunnels
   c) Extending Wi-Fi range
   d) Identifying connected devices

11. Which attack disrupts a network by flooding it with excessive traffic?
   a) Eavesdropping
   b) Man-in-the-middle (MITM) attack
   c) Denial of Service (DoS)
   d) Spoofing

12. What is the main advantage of using 802.1X authentication in enterprise networks?
   a) Open access to all users
   b) Simple setup process
   c) Secure user authentication
   d) Increased bandwidth

13. What principle is violated in a Man-in-the-Middle (MITM) attack?
   a) Confidentiality
   b) Availability
   c) Scalability
   d) Speed

14. Which of the following best describes a Wireless Mesh Network (WMN)?
   a) A single access point providing coverage
   b) Multiple interconnected nodes sharing network access
   c) Satellite-based communication system
   d) Device-to-device pairing using Bluetooth

15. What is the primary role of encryption in wireless security?
   a) Ensuring network availability
   b) Preventing unauthorized modifications
   c) Securing data during transmission
   d) Detecting anomalies in the network

B. Fill in the Blanks

1. _____ encryption provides the highest level of security for Wi-Fi networks.
2. A _____ intercepts and listens to wireless communications.
3. An unauthorized access point set up to mimic a legitimate one is known as a _____.
4. _____ networks cover broad areas using cellular technology.
5. _____ attack involves flooding the network with traffic, causing service disruptions.
6. _____ provides strong encryption and authentication for Wi-Fi networks.
7. _____ use radio waves to connect devices without physical cables.
8. Wireless networks rely on _____ signals to transmit data.
9. The _____ protocol is widely used for Wi-Fi networks.
10. A _____ creates secure tunnels for transmitting data over public networks.
11. _____ authentication uses RADIUS servers for secure access control.
12. Devices in a Wireless Personal Area Network typically use _____ or Zigbee.

C. True or False

1. WLAN stands for Wireless Local Area Network.
2. WPA3 is the latest and most secure Wi-Fi security protocol.
3. Changing default passwords is a recommended practice for improving wireless network security.
4. Disabling WPS can improve wireless network security.
5. VPNs create secure connections by encrypting data over the internet.
6. WPA2 is weaker than WEP in terms of security.
7. Wireless networks are immune to Denial of Service (DoS) attacks.
8. WPA2 is considered insecure for modern wireless networks.
9. A VPN provides encrypted communication over wireless networks.
10. Wireless networks are immune to signal interference.
11. Eavesdropping can compromise the confidentiality of a wireless network.
12. Wireless Mesh Networks are ideal for disaster recovery scenarios.
13. Firewalls are unnecessary for wireless security.
14. 802.1X authentication is commonly used in enterprise environments.

D. Short Answer Questions

1. What are the types of wireless networks, and what areas do they cover?
2. How does an access point (AP) function in a wireless network?
3. What are common wireless security threats, and how do they affect networks?
4. Explain the difference between WPA2 and WPA3 security protocols.
5. List two advantages and two disadvantages of wireless networks.

E. Long Answer Questions

1. Discuss the importance of wireless network security and the common threats faced by wireless networks. Provide examples of how these threats can impact users.
2. Describe the various wireless security protocols (WEP, WPA, WPA2, WPA3) and their evolution. Explain the strengths and weaknesses of each protocol.
3. Discuss the key security risks in wireless networks and suggest methods to mitigate them. Explain the best practices for securing a wireless network.
4. Explain the concept of a Wireless Mesh Network (WMN) and its applications in modern technology.

ANSWER KEY

A. Multiple Choice Questions

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

B. Fill in the Blanks

1.WPA3, 2.Eavesdropper, 3.Rogue access point, 4.WWAN, 5.Denial of Service (DoS), 6.WPA3, 7.Wireless networks, 8.Radio, 9.IEEE 802.11, 10.VPN, 11.802.1X, 12.Bluetooth

C. True or False

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

Chapter-6

Mobile OS Security (Android and iOS)

Rahul: (smiling) Neha, when will you finally switch to Android? It's clearly better!

Neha: (laughing) Not happening, Rahul. My iPhone is perfect for me. But go on, what's so great about Android?

Rahul: Customization! I can tweak my home screen, add widgets, and install apps Apple won't allow.

Neha: I prefer iOS for its simplicity. Everything is organized and just works smoothly.

Rahul: But Android gives more options—phones at every price with diverse features. Apple is so limited.

Neha: True, but that's why iPhones work seamlessly and last longer.

Rahul: Android still wins with better hardware, like my 200MP camera and fast charging.

Neha: My iPhone takes amazing pictures, and iOS is unmatched for video recording.

Rahul: Okay, but Android has split-screen multitasking and USB-C charging. No Lightning cable hassle!

Neha: USB-C is great, but iPhones get instant updates and better privacy features.

Rahul: Fair, but Android innovates first, and Google Assistant is leagues ahead of Siri.

Neha: Siri does need improvement, but iMessage and FaceTime are unbeatable.

Rahul: iMessage is great, but Android works better with apps like WhatsApp for everyone.

Neha: (smiling) We just value different things—I love Apple's ecosystem, and you love Android's variety.

Rahul: (raising his chai) Cheers to that, Neha. At least we agree on chai!

Neha: (clinking her cup) Cheers. Maybe one day, we'll get a phone with the best of both worlds.

Both Android OS and iPhone iOS have carved out their niches in the mobile market. Android offers flexibility and affordability, while iOS is tailored for security and seamless integration within the Apple ecosystem. Users should weigh their priorities, such as customization or security, before choosing the OS that best suits their needs.

6.1 Introduction to Android OS and iPhone iOS

In the world of smartphones, the two leading mobile operating systems, Android OS and iPhone iOS, dominate the global smartphone market. Mobile operating systems (OS) are essential for managing hardware resources and providing an interface for users to interact with devices. Two of the most popular mobile operating systems are Android OS and iPhone iOS, both offering unique capabilities and ecosystems.

- **Android OS:** Android OS was developed by Google. It is an open-source operating system built on the Linux kernel. It powers a wide variety of devices, offering high customizability, scalability, and compatibility. Android's flexibility makes it popular among manufacturers. It was primarily designed for touchscreen devices. It supports a vast range of devices from various manufacturers, such as Samsung, OnePlus, and Xiaomi.

Figure 6.1 Android Robot Logo Author: https://developer.android.com/

- **iPhone iOS:** It was developed by Apple, iOS is a proprietary mobile operating system exclusively designed for Apple devices such as the iPhone, iPad, and iPod Touch. Known for its seamless performance and integration with Apple's ecosystem, iOS prioritizes security, aesthetics, and user experience. iOS emphasizes a polished user experience and tight control over hardware and software.

These both operating systems power the vast majority of mobile devices, providing the foundation for apps, communication, entertainment, and more. Understanding their specializations, features, components, and security aspects is essential for anyone interested in mobile technology.

Figure 6.2 iOS 18 Logo Author: https://www.apple.com/in/ios/ios-18/

6.2 Specialization and Key Features of Android OS

Android OS is characterized by its adaptability, customization, and compatibility with a wide range of hardware. Android excels in adaptability, making it suitable for diverse markets and price points. Its modularity enables manufacturers to create unique user experiences tailored to different demographics. Android OS offers diverse capabilities that make it adaptable for various user needs and device types. (*Figure 6.3)*

- **Open Source:** Android's open-source nature allows manufacturers to customize it according to their needs.

  Example: Samsung's One UI and Xiaomi's MIUI are custom Android interfaces.

- **Customizable:** Android users can modify their home screens using widgets, custom themes, launchers, and even the system interface through third-party apps or ROMs.

Example: Samsung's One UI offers a distinct look compared to Google's Pixel interface.

- **Device Variety and Wide Hardware Support:** Android powers budget smartphones to high-end devices, providing consumers with options at various price points. Supports a variety of devices, from budget-friendly models to premium flagship smartphones. Android is compatible with a wide range of hardware, including foldable phones, smart TVs, and wearables. **Example:** Devices range from affordable Xiaomi Redmi phones to premium Samsung Galaxy models.

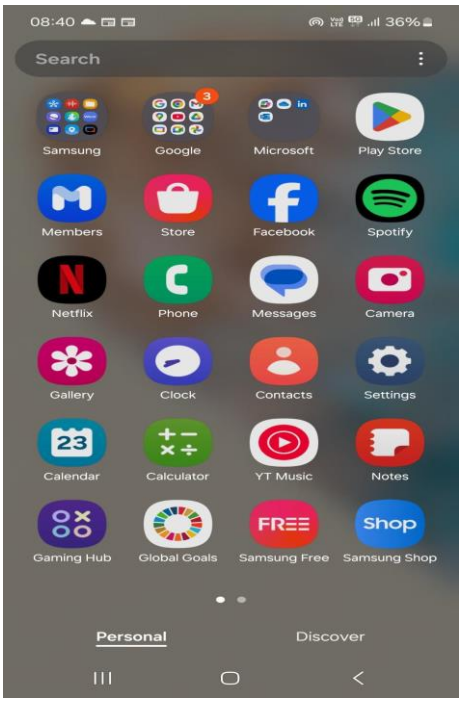


Figure 6.3 Android Apps Interface

- **Google Ecosystem Integration:** Seamless integration with Google services like Gmail, Google Drive, Google Maps, Google Photos, and Google Assistant. **Example:** Android users can sync their files and apps across devices using Google Drive.(*Figure 6.4)*

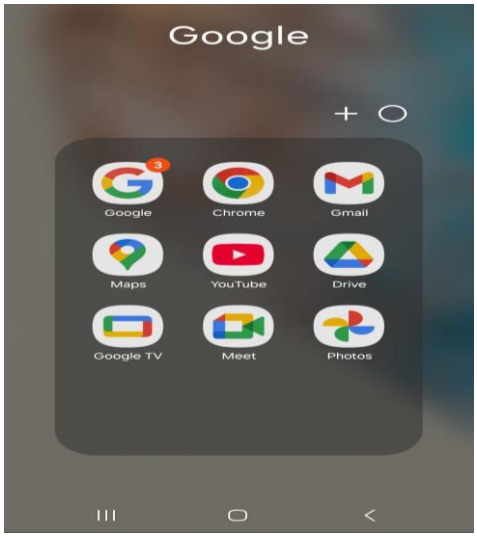


Figure 6.4 Google Ecosystem Integration

- **Google Play Store:** Access to millions of apps on the Google Play Store, catering to diverse needs from productivity to entertainment and ensuring diversity in app availability.
- **Third-Party App Stores:** In addition to the Google Play Store, users can download apps from other sources.

  Example: Amazon Appstore or Huawei AppGallery.
- **Multitasking and Notifications:** Supports split-screen and robust notification systems for enhanced productivity.

  Example 1: Split-screen mode allows users to run two apps side by side, improving productivity and convenience.

  Example 2: Rich notifications provide quick actions, replies, and detailed information without opening the app.
- **Expandable Storage and Hardware Support:** Android supports external storage (microSD) and hardware peripherals like USB drives.
- **Voice Commands:** Google Assistant enables voice commands for tasks such as setting reminders, sending messages, or controlling smart home devices.

6.3 Basic Components of Android OS

Android's architecture is built to ensure scalability and performance. It has the following key components.(*Figure 6.5)*

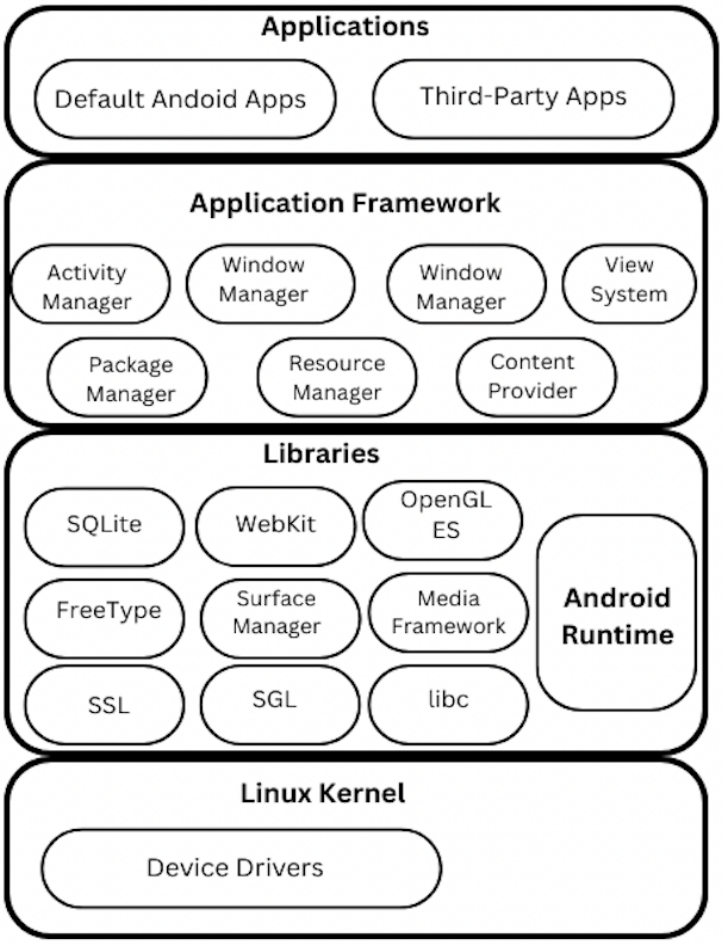


Figure 6.5 Android OS Components

1. **Applications:** These are User-facing software known as apps that provide specific functionalities. The top layer where users interact with apps like messages, email, and games.

   Example: Apps like Gmail, Camera, and Chrome run on top of the Android stack. The other apps are like Social media apps, games, and productivity tools.

2. **Application Framework:** It provides reusable components like Activities, Services, Broadcast Receivers, and Content Providers. Also, provides APIs for developers to create applications.

   Example: Content providers, resource managers, view systems. Activities manage a single screen of an app, like the login screen of Facebook. Activity Manager handles app lifecycle.

3. **Libraries:** Android uses a set of core libraries which are precompiled code for data storage, graphics rendering, and media playback. It provides fundamental capabilities.

   Example: SQLite is used for database management, Graphics libraries

4. **Android Runtime**: It is pre-written code. It converts app code into machine-readable code for execution, and ensures memory management and smooth performance.

   Example: data storage, web browsers.

5. **Linux Kernel:** It acts as the core of the OS, managing hardware resources and providing security. It is the core system component that manages hardware and system resources.

   Example: Memory management, security settings, process management.

6.4 Security Features and Threats in Android OS

6.4.1 Security Features

1. **Google Play Protect:** It scans apps for malware and protects against threats avoiding harmful behavior.

   Example: Automatically scans downloaded apps and alerts users if any issues are found.

2. **Application Sandbox:** Sandboxing feature isolates apps to prevent them from accessing each other's data. Apps run in isolated environments, preventing unauthorized access to other apps' data.

   Example: A game app cannot access the user's contact information unless explicitly granted permission.

3. **Permissions System:** Users must grant explicit permissions for sensitive actions.

   Example: Camera or location access.

4. **Encryption:** Data is encrypted by default on modern Android devices to protect it from unauthorized access.

   Example: Full-disk encryption ensures that data remains secure even if the device is lost or stolen.

5. **Biometric Authentication:** Uses fingerprints or facial recognition to unlock devices and apps.

Example: Unlocking the phone using a fingerprint scanner.

6.4.2 Security Threats

1. **Malware and Ransomware:** Due to the open nature, rogue apps may infiltrate via third-party stores.

   Example: Fake apps designed to steal data. Malicious apps that steal personal information or cause damage to the device.

2. **Phishing Attacks:** Social engineering attacks trick users into revealing sensitive information.

   Example: Fake websites or apps that trick users into providing sensitive information.

3. **Unsecured Wi-Fi:** Hackers intercepting data transmitted over public Wi-Fi networks.
4. **Outdated Software:** Fragmentation can lead to devices not receiving timely security patches.

   Example: Security vulnerabilities in older versions of the OS that haven't been patched.

5. **Rooting Risks:** Modifying the OS can expose vulnerabilities.

Points to Remember:

Android OS, developed by Google, is an open-source, versatile, and widely used across various devices.

iOS, developed by Apple, is proprietary, emphasizing security, seamless integration, and performance.

Android OS is:

- Open-source, highly customizable with widgets, themes, and third-party app support.
- Features include Google integration, app availability, multi-tasking, rich notifications, voice commands and foldable displays.
- Wide device range, from budget-friendly to premium models.

Basic Components of Android

- Applications
- Application Framework
- Libraries
- Android Runtime (ART)
- Linux Kernel

Security Features of Android

- Google Play Protect, application sandbox, encryption, biometric authentication.

Security Threats of Android

Malware, phishing, unsecured Wi-Fi, outdated software.

6.5 Specialization and Features of iPhone iOS

iPhone iOS, developed by Apple, is known for its smooth user experience, robust security features, and seamless integration with Apple's ecosystem. iOS is renowned for its seamless integration and strict quality controls. iOS specializes in delivering a premium experience with unparalleled security and consistent updates. It is particularly appealing to users invested in the Apple ecosystem. Apple's iOS stands out for its unified design, optimization, and focus on user experience.

6.5.1 Key Features of iPhone iOS

- **Optimized Performance:** Tight hardware-software integration ensures fluid operation. iOS updates are available to all compatible devices simultaneously.

Figure 6.6 Apple's App Store

- **App Store:** Strict app approval process minimizes malicious app risks. A strict app review process ensures high-quality and secure apps. Apple's App Store prioritizes security and quality, ensuring all apps meet strict guidelines. (*Figure 6.6)*
- **User Interface (UI):** Known for simplicity and elegance. Intuitive and consistent design, making it easy for users to navigate and use their devices.(*Figure 6.7)*

Figure 6.7 Apple's UI

- **Siri:** An advanced voice assistant for automation and information retrieval. Voice-activated assistant that can perform tasks such as sending messages, setting alarms, and providing information.

Figure 6.8 Siri

- **Continuity:** Seamless integration across Apple devices, allowing users to start a task on one device and continue on another.
- **Privacy Controls and Security:** Features like App Tracking Transparency allow users to control which apps can track their activity.

  iOS emphasizes user data protection with features like App Tracking Transparency and secure facial recognition (*Figure 6.9*). **Example:** Apps must ask for permission before tracking user data.

Figure 6.9 iphone iOS interface

- **Unified Ecosystem:** iOS devices work seamlessly with other Apple products like Macs, iPads, and Apple Watches.

  Example: Handoff allows users to start a task on an iPhone and continue it on a Mac.
- **Regular Updates:** Apple provides regular updates to all supported devices, ensuring long-term performance and security. Regular software updates provided directly by Apple ensure all devices receive the latest features and security patches.
- **Exclusive Features:** Includes features like FaceTime, iMessage, and AirDrop for Apple ecosystem users which enhance communication and file-sharing among iOS users.

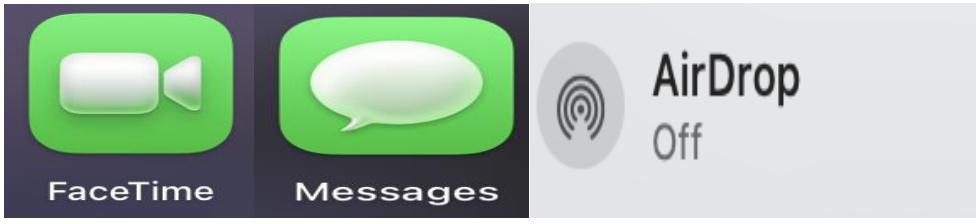


Figure 6.10 iOS Features FaceTime, iMessage and AirDrop

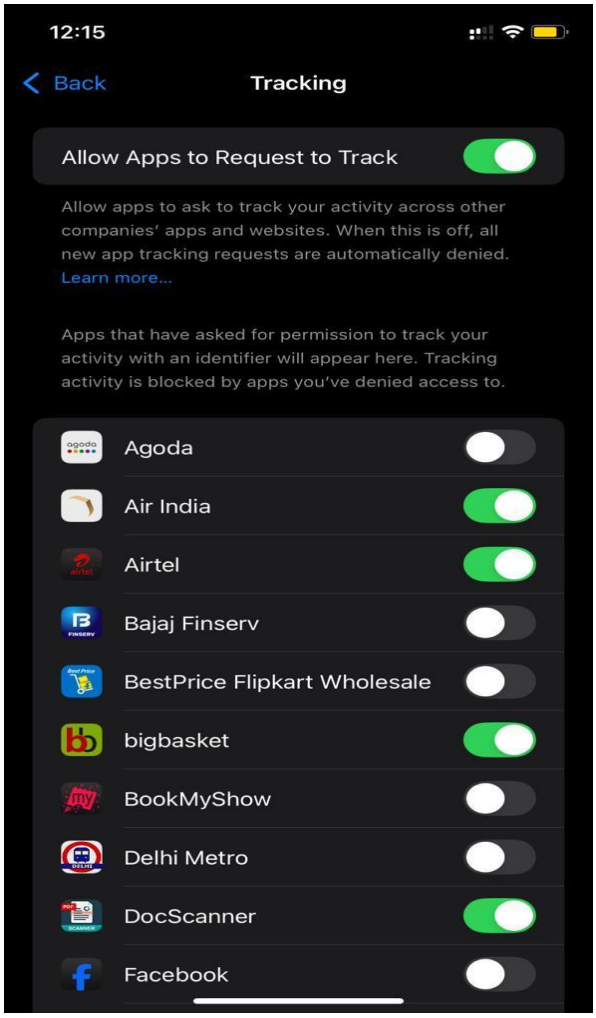


Figure 6.11 App Tracking in iOS

6.5.2 Basic Components of iOS

iOS architecture ensures reliability and performance across Apple devices. It has the following key components(*Figure 6.12)*:

- **Core OS Layer:** It provides low-level functionality, including file system access and security. It ensures secure boot and file encryption.
- **Core Services Layer:** It offers essential services like location tracking and networking. For example, Core Location API helps apps determine a device's location.
- **Media Layer:** It handles graphics, audio, and video playback. It has AVFoundation for video playback in apps like YouTube.
- **Cocoa Touch Layer:** It supports multi-touch gestures, notifications, and app lifecycle management. It has a UIKit framework that enables interface elements like buttons and tables.
- **Applications:** iOS applications are optimized for seamless performance, including pre-installed apps like Safari and Messages.

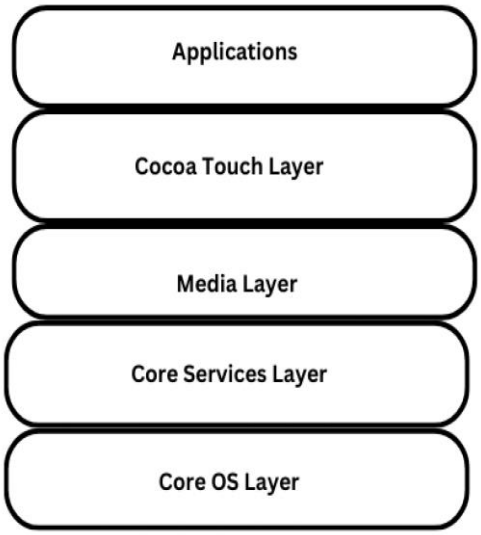


Figure 6.12 Basic Components of iOS

6.6 Security Features and Security Threats of iOS

6.6.1 Security Features

- **App Sandbox:** Apps have restricted access to the system and user data.
- **App Review Process:** Rigorous review process for apps submitted to the App Store. Apps are reviewed for security, privacy, and functionality before being approved.
- **Data Encryption:** It encrypts data on the device and in transit to protect user information and communication. End-to-end encryption protects all sensitive data.

  Example: iMessage encrypts messages end-to-end, ensuring only the sender and the receiver can read them.
- **Biometric Authentication:** It uses Face ID or Touch ID to unlock devices and authorize transactions for secure access.

  Example: Using Face ID to authenticate a payment through Apple Pay.
- **Secure Enclave:** A dedicated chip that handles sensitive data like encryption keys and biometric information.

  Example: Face ID data is stored securely in the Secure Enclave.
- **Find My:** Allows users to locate, lock, or wipe their devices remotely.(*Figure 6.13)*

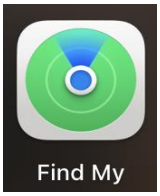


Figure 6.13 Find My feature in iOS

- **Regular Updates:** Apple ensures devices receive timely security patches.
- **Privacy & Security:** It provides safety check, sensitive content warning, App privacy report, stolen device protection and lockdown mode. (Figure 6.14)

6.6.2 Security Threats

- **Malicious Apps:** Although rare due to the app review process, some malicious apps may slip through and compromise user data.
- **Supply Chain Attacks:** In this attack malicious code introduced during app development.
- **Phishing:** Fake emails or messages that attempt to trick users into providing personal information.

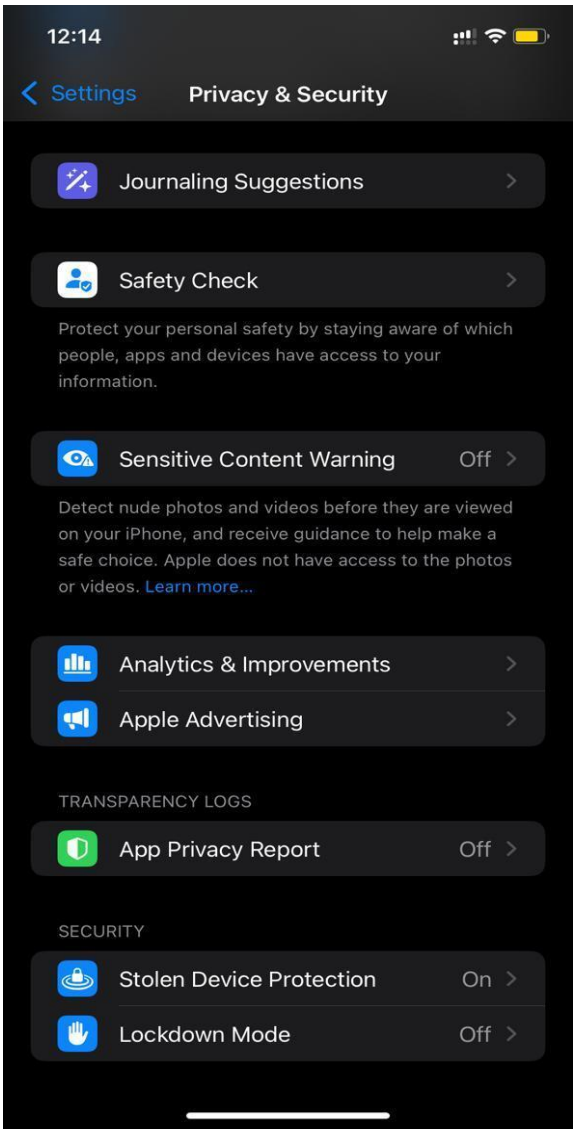


Figure 6.14 Privacy & Security-iOS

- **Zero-Day Vulnerabilities**: These are exploits that take advantage of unknown vulnerabilities in the OS before they are patched. Rare, but exploits can affect devices before patches are available.
- **Social Engineering Attacks:** These are scams targeting Apple ID credentials. Manipulating users into giving up sensitive information through deceitful tactics like lucrative audio and video calls.
- **Jailbreaking Risks:** Similar to Android rooting, jailbreaking compromises security.

Points to Remember:

Specialization and Features of iOS

- Unified ecosystem with seamless integration across Apple devices.
- Privacy-focused with features like App Tracking Transparency and Face ID.
- Regular updates and exclusive features like iMessage, FaceTime, Handoff, App Store, Siri, continuity, and privacy controls.
- known for smooth user experience and robust security.

Basic Components of iOS

- Cocoa Touch: Manages user interface and multitouch gestures.
- Media Layer: Handles audio, video, and graphics.
- Core Services: Provides APIs for location, networking, and storage.
- Core OS: Handles low-level functionalities like security and file system.
- Pre-installed Apps: Optimized tools like Safari and Messages.

Security Features of iOS

- App review process, data encryption, biometric authentication, Secure Enclave.

Security Threats of iOS

Malicious apps, phishing, zero-day vulnerabilities, social engineering.

Practical Activity 6.1

Objective: Learners will set up and test biometric authentication (fingerprint or facial recognition) on an Android device.

Tools & Platform Needed: Android smartphone or tablet with biometric authentication capability

Group Formation and Task Assignment:

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

Step 2. Assign each group either fingerprint or facial recognition set up and testing task

Procedure to Set Up Fingerprint Authentication:

Step 1. Open the "Settings" app on an Android device.

Step 2. Choose "Fingerprint" and follow the on-screen instructions to register a fingerprint.

Step 3. Select "Security & location" or "Biometrics & security."

Step 4. Place your finger on the fingerprint sensor multiple times until the fingerprint is registered.

Step 5. Set up a backup PIN or password in case the fingerprint sensor fails.

Procedure to Set Up Facial Recognition Authentication:

Step 1. Open the "Settings" app on an Android device.

Step 2. In the same "Security & location" or "Biometrics & security" menu, select "Face unlock" or "Facial recognition."

Step 3. Follow the on-screen instructions to register your face.

Step 4. Ensure your face is well-lit and fully visible during the registration process.

Procedure to Test Biometric Authentication:

Step 1. Lock Android device using the above mentioned authentication and then unlock it using the registered fingerprint or facial recognition.

Step 2. Test the biometric authentication multiple times to ensure reliability.

Document the process:

Each group will showcase their findings in the form of presentation slides in front of class and discuss the importance of Biometric Authentication and their impact on personal information security.

Practical Activity 6.2

Objective: Learners will configure and manage app permissions on an Android/iPhone to control access to sensitive information and device features.

Tools & Platform Needed: Android/iphone smartphone or tablet/ipad

Procedure:

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

Step 2. Assign each group configure and manage app permissions

Step 3. Open the "Settings" app on an Android/iPhone device.

Step 4. Scroll down and select "Privacy."

Step 5. Choose a category (e.g., Location Services, Camera, Microphone).

Step 6. Select an app from the list to see its current permissions.

Step 7. Toggle the permissions on or off based on your preferences.

Step 8. For location services, you can choose between "Never," "Ask Next Time," "While Using the App," or "Always."

Step 9. Check apps permission by opening various apps that require permissions (e.g., maps, camera, social media).

Step 10. Pay attention to the prompts requesting access to location, camera, microphone, etc.

Step 11. Decide whether to grant or deny permissions based on the app's functionality and your privacy concerns.

Document the above steps and findings: Each group will showcase their findings in the form of presentation slides in front of class and discuss the importance of Biometric Authentication and their impact on personal information security.

List of other suggested practicals and activities:

- **Digital Wellbeing and Screen Time Test:**

  Objective: Monitor app usage and digital habits to Awareness of digital habits and productivity.

Activities: Use built-in tools like Digital Wellbeing (Android) or Screen Time (iOS) to analyze daily device usage.

- **Backup and Restore Data Practice:**

  Objective: Ensure data safety through backups Knowledge of backup practices

  Activities: Demonstrate how to back up data on Google Drive (Android) and iCloud (iOS).

- **Software Updates and Security Patches:**

  Objective: Understand the importance of software updates keeping devices up-to-date.

  Activities: Check the latest software updates on Android and iOS devices and explain how updates patch vulnerabilities.

- **Usage of Find my device apps for device and data safety:**

  Objective: Locating attached devices on google map and apple map to ensure the safety of devices and monitor its appropriate use.

  Activities: Access Find my device apps on android and iphone devices. Sign in with gmail/apple id and track on map.

Summary

Introduction

- Android OS, developed by Google, is open-source, versatile, and widely used across various devices.
- iOS, developed by Apple, is proprietary, emphasizing security, seamless integration, and performance.
- Android OS and iPhone iOS dominate the smartphone market.

Specialization and Features of Android OS

- Open-source, highly customizable with widgets, themes, and third-party app support.
- Features include Google integration, app availability, multi-tasking, rich notifications, and voice commands.
- Wide device range, from budget-friendly to premium models.
- Google services integration and compatibility with advanced technologies like foldable displays.

Specialization and Features of iOS

- Unified ecosystem with seamless integration across Apple devices.
- Privacy-focused with features like App Tracking Transparency and Face ID.
- Regular updates and exclusive features like iMessage, FaceTime, and Handoff.
- known for smooth user experience and robust security.
- Features include user interface, App Store, Siri, continuity, privacy controls, and regular updates.

Basic Components of Android

- Applications: End-user tools like Gmail and Chrome.

- Application Framework: APIs for developers, Components like Activities, Services, and Broadcast Receivers.
- Libraries: Support multimedia, database, and graphics.
- Android Runtime (ART): Executes app code.
- Linux Kernel: Manages hardware and system resources.
- Applications: User-facing software.

Basic Components of iOS

- Cocoa Touch: Manages user interface and multitouch gestures.
- Media Layer: Handles audio, video, and graphics.
- Core Services: Provides APIs for location, networking, and storage.
- Core OS: Handles low-level functionalities like security and file system.
- Pre-installed Apps: Optimized tools like Safari and Messages.

Security Features and Security Threats of Android

- Security Features: Google Play Protect, application sandbox, encryption, biometric authentication.
- Security Threats: Malware, phishing, unsecured Wi-Fi, outdated software.

Security Features and Security Threats of iOS

- Security Features: App review process, data encryption, biometric authentication, Secure Enclave.
- Security Threats: Malicious apps, phishing, zero-day vulnerabilities, social engineering.

ASSESSMENT

A. Multiple Choice Questions

1. Who developed Android OS?
   a) Apple
   b) Google
   c) Microsoft
   d) Samsung

2. Which layer in iOS handles graphics and multimedia?
   a) Cocoa Touch
   b) Core Services
   c) Media Layer
   d) Core OS

3. What is the base kernel of Android OS?
   a) Unix
   b) Linux
   c) Windows
   d) macOS

4. What feature in iOS protects user privacy by controlling app tracking?
   a) Secure Boot
   b) App Tracking Transparency

c) Core Location
d) Handoff

5. Which Android feature allows devices to act as desktops?
   a) Google Assistant
   b) Android Runtime
   c) Samsung DeX
   d) ART

6. iOS applications are primarily managed using which framework?
   a) ART
   b) UIKit
   c) SQLite
   d) OpenGL ES

7. Which component in Android handles 3D rendering?
   a) SQLite
   b) OpenGL ES
   c) ART
   d) Services

8. What is the primary purpose of the Linux Kernel in Android?
   a) File management
   b) App updates
   c) Hardware resource management
   d) UI rendering

9. What is an exclusive feature of iOS?
   a) FaceTime
   b) Widgets
   c) Custom ROMs
   d) Google Play Store

10. Which Android component provides tools for app development?
    a) Media Layer
    b) Application Framework
    c) Core OS
    d) AVFoundation

B. Fill in the Blanks

1. Android OS is based on the _____ kernel.
2. iOS is a _____ operating system developed by Apple.
3. _____ allows Android users to modify their home screens and themes.
4. The _____ framework in iOS manages the app lifecycle and user interface.
5. _____ is an Android runtime environment that converts app code into machine-readable code.
6. _____ is an exclusive Apple feature for encrypted messaging.
7. The _____ layer in iOS handles location and networking services.

8. _____ allows iOS users to transfer tasks between Apple devices seamlessly.
9. The _____ component in Android OS handles multimedia playback and graphics rendering.
10. _____ in Android provides APIs for app development like Activities and Services.

C. True/False

1. Android OS is a closed-source operating system.
2. iOS updates are available for all supported Apple devices, including older models.
3. OpenGL ES is used for 3D rendering in iOS.
4. FaceTime is a unique feature of Android OS.
5. Google Play Store is the only app store available on Android devices.
6. iOS is optimized specifically for Apple hardware.
7. The Linux Kernel in Android manages system hardware resources.
8. The Cocoa Touch layer in iOS provides support for multitouch gestures.
9. App Tracking Transparency is a feature exclusive to Android.
10. Android allows users to sideload apps from external sources.

D. Short Answer Questions

1. What are the core differences between Android OS and iOS in terms of openness and ecosystem?
2. Mention two key features that make Android highly customizable.
3. What is the role of the Linux Kernel in Android?
4. Highlights key security features of Android OS?
5. Name two key features of iOS that ensure user privacy.
6. What is the purpose of the Cocoa Touch layer in iOS?
7. Mention one example of hardware supported by Android that iOS doesn't yet accommodate.
8. How does Google Play Protect enhance security in Android devices?
9. Explain the purpose of biometric authentication in mobile operating systems.

E. Long Answer Questions

1. Compare and contrast the specialization and features of Android OS and iOS.
2. Explain the basic components of Android OS and their security functions with examples.
3. Describe the architecture of iOS and how its components ensure efficiency and security.
4. Discuss the security threats in Android OS with examples.
5. Explain the application framework in Android OS and its major components.
6. Discuss the customization and features of Android OS that make it popular among users. Provide examples to support your points.
7. Explain the security features and potential threats of iPhone iOS. How does Apple address these threats to ensure user data protection?

ANSWER KEY

A. Multiple Choice Questions

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

B. Fill in the Blanks

1.Linux, 2.closed-source, 3.Customization, 4.UIKit, 5.ART, 6.iMessage, 7.Core Services, 8.Handoff, 9.Media Framework, 10.Application Framework

C. True or False

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

Chapter-7

Web Application Protocols and Browser Security

Anand ran a thriving organic skincare brand from Coimbatore. His handmade soaps and herbal lotions had earned a loyal customer base, and he recently launched an e-commerce website to manage growing demand. The site allowed users to browse products, place orders, and subscribe to newsletters. Business was booming, and Anand felt proud—his dream had gone digital.

One morning, he received a distressed message from a regular customer. Their credit card had been charged for items they never ordered, and they'd received a suspicious email asking for their address and Aadhaar number. Anand was shocked. He hadn't sent any such email.

Worried, he called his cousin Karthik, a cybersecurity analyst. Karthik examined the website and uncovered a serious breach: hackers had exploited an outdated plugin to inject malicious code. Customers were being redirected to a fake checkout page that harvested payment details and personal information.

Anand had assumed his small business wouldn't be a target. He hadn't installed a firewall, enabled HTTPS, or updated his CMS. "It's just soap," he had once joked. But now, his customers' trust was shaken, and he faced penalties under India's IT Act for mishandling sensitive data.

The irony was painful—Anand, who built his brand on purity and wellness, had unknowingly exposed his customers to digital harm. He shut down the site temporarily, hired a security firm, and launched an awareness campaign to educate his customers about online safety.

From that day forward, Anand became a vocal advocate for cybersecurity in small businesses. His story became a lesson in digital hygiene—because even the cleanest brands can be compromised if they don't protect themselves online.

7.1 Web Application Components

Web applications are dynamic platforms that allow users to interact with services through a browser. They consist of several interconnected components:

- **Client-side (Frontend)**: Built using HTML, CSS, and JavaScript, this layer handles user interface and interactions.
- **Server-side (Backend)**: Processes business logic, handles authentication, and communicates with databases. Technologies include Node.js, Python, PHP, and Java.
- **Database**: Stores user data, content, and transactional records. Examples include MySQL, PostgreSQL, and MongoDB.
- **Web Server**: Hosts the application and serves content to users. Common servers include Apache and Nginx.
- **API (Application Programming Interface)**: Facilitates communication between frontend and backend or with third-party services.

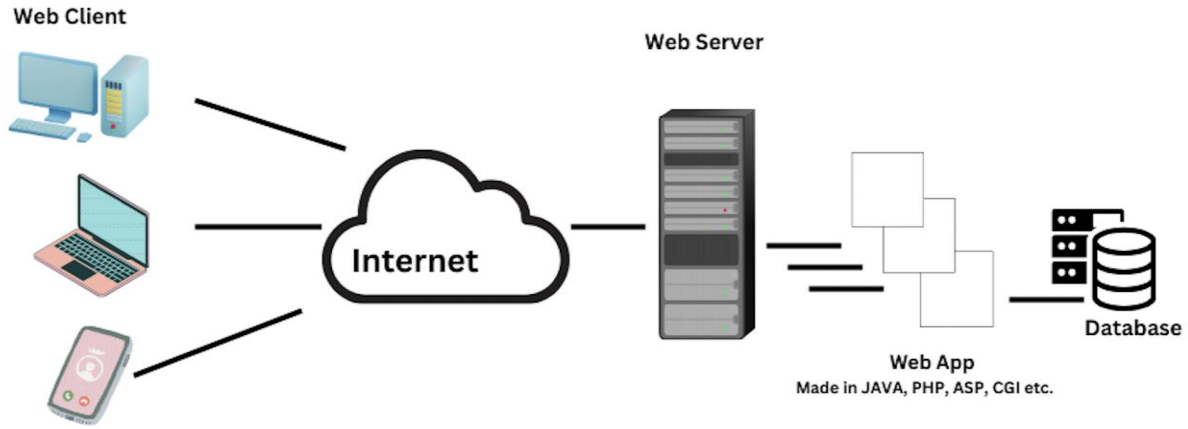


Fig 7.1 Web Application Components

Each component plays a critical role in delivering a seamless user experience—and each must be secured to prevent exploitation(Fig 7.1).

7.2 Protocols: HTTP vs HTTPS

The **HTTP (HyperText Transfer Protocol)** is the foundation of web communication, enabling data exchange between browsers and servers. However, HTTP transmits data in plaintext, making it vulnerable to interception and manipulation. It uses port 80 for communication.

To address this, **HTTPS (HTTP Secure)** was introduced. HTTPS uses **SSL (Secure Sockets Layer)** or its successor **TLS (Transport Layer Security)** to encrypt data in transit. This ensures:

- **Confidentiality**: Data is unreadable to unauthorized parties.
- **Integrity**: Data cannot be altered during transmission.
- **Authentication**: Verifies the identity of the server.

HTTPS operates over port 443 and is now a standard for any website handling sensitive information like login credentials or payment details.

7.3 SSL/TLS: The Backbone of Secure Communication

SSL and TLS are cryptographic protocols that secure online communication. While SSL is largely deprecated, TLS (especially versions 1.2 and 1.3) is widely used today. These protocols use certificates issued by trusted Certificate Authorities (CAs) to validate server identities and establish encrypted connections.

To evaluate a website's HTTPS configuration, tools like **SSL Labs** are invaluable. By entering a domain into SSL Labs, users can assess:

- Certificate validity and expiration
- Supported TLS versions
- Cipher strength and key exchange mechanisms
- Vulnerabilities like Heartbleed or weak configurations

This kind of analysis helps developers and security professionals ensure that their websites meet modern security standards.

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.

7.4 Secure Browsing Practices

Safe browsing is essential for protecting personal data and avoiding cyber threats. Recommended practices include:

- Always verify that websites use **HTTPS** before entering sensitive information.
- Avoid clicking on suspicious links, pop-ups, or email attachments.
- Keep browsers and extensions updated to patch known vulnerabilities.
- Use **ad blockers**, **anti-tracking tools**, and **VPNs** for added privacy.
- Enable **Safe Browsing** features in browser settings to detect phishing and malware.
- Avoid conducting financial transactions over public Wi-Fi unless using a secure VPN.

These habits form the first line of defense against online threats.

7.5 Cookies and Session Management

Cookies are small data files stored in the browser to maintain user state across sessions. They are used for:

- Authentication (e.g., login sessions)
- User preferences (e.g., language settings)
- Tracking (e.g., analytics and advertising)

Session management ensures that users remain authenticated across multiple requests. Common techniques include:

- **Session IDs** stored in cookies
- **Tokens** such as JWT (JSON Web Tokens)

To secure sessions:

- Use **Secure** and **HttpOnly** flags to prevent access via JavaScript.
- Set the **SameSite** attribute to mitigate CSRF attacks.
- Implement **session expiration** and **logout mechanisms**.
- Avoid storing sensitive data in cookies.

Poor session management can lead to vulnerabilities like **session hijacking**, where attackers steal session tokens to impersonate users.

7.6 Chrome Browser Security Settings: A Practical Demonstration

Google Chrome offers robust security settings to help users protect their browsing experience. To access them:

1. Open Chrome → Click ⋮ → Settings → Privacy and Security

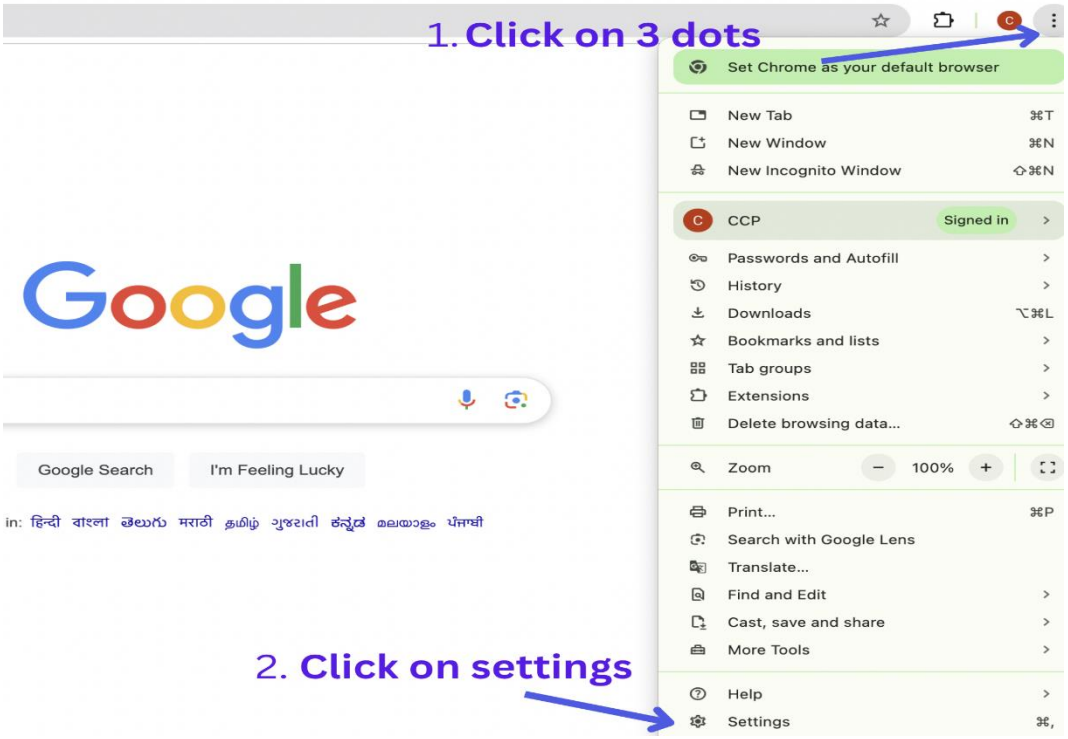


Figure 7.2 Accessing Chrome Browser Settings Step 1 & 2

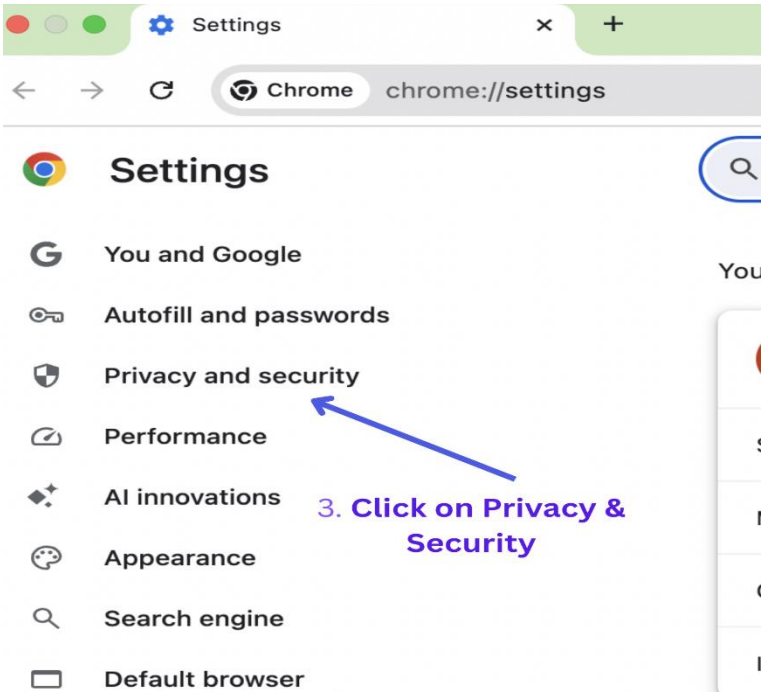


Figure 7.3 Accessing Chrome Browser Settings Step 3

2. Key options include:
    - **Safe Browsing**: Choose between Standard and Enhanced Protection(Fig 7.4 & 7.5).

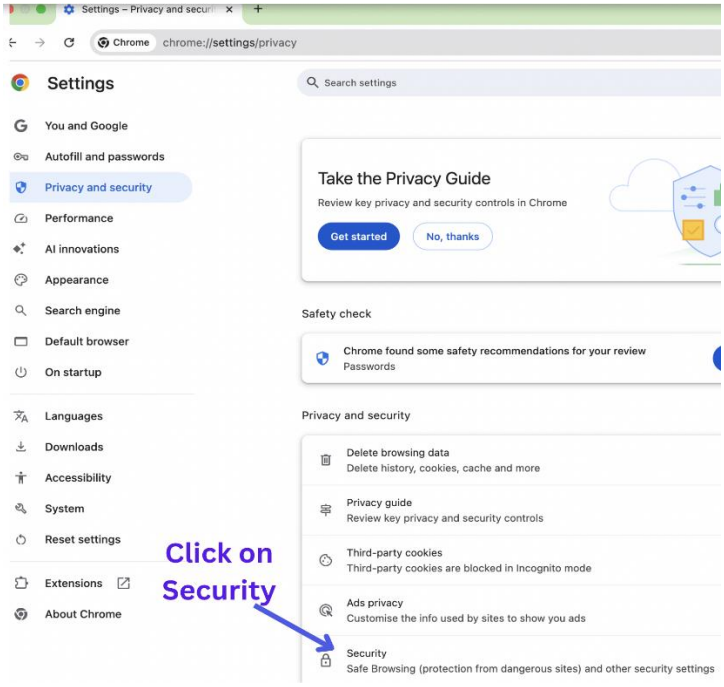


Figure 7.5 Accessing Chrome Browser Security for Safe Browsing

    - **Site Settings**: Control access to cookies, location, camera, and microphone (Fig 7.6).
    - **Clear Browsing Data**: Remove cookies, cache, and history.
    - **Security**: Enable HTTPS-only mode and manage certificates.

These settings empower users to customize their privacy and security preferences.

7.7 Using Chrome Developer Tools to Inspect Cookies and Headers

Chrome DevTools is a powerful tool for inspecting how websites handle cookies and headers. To access it:

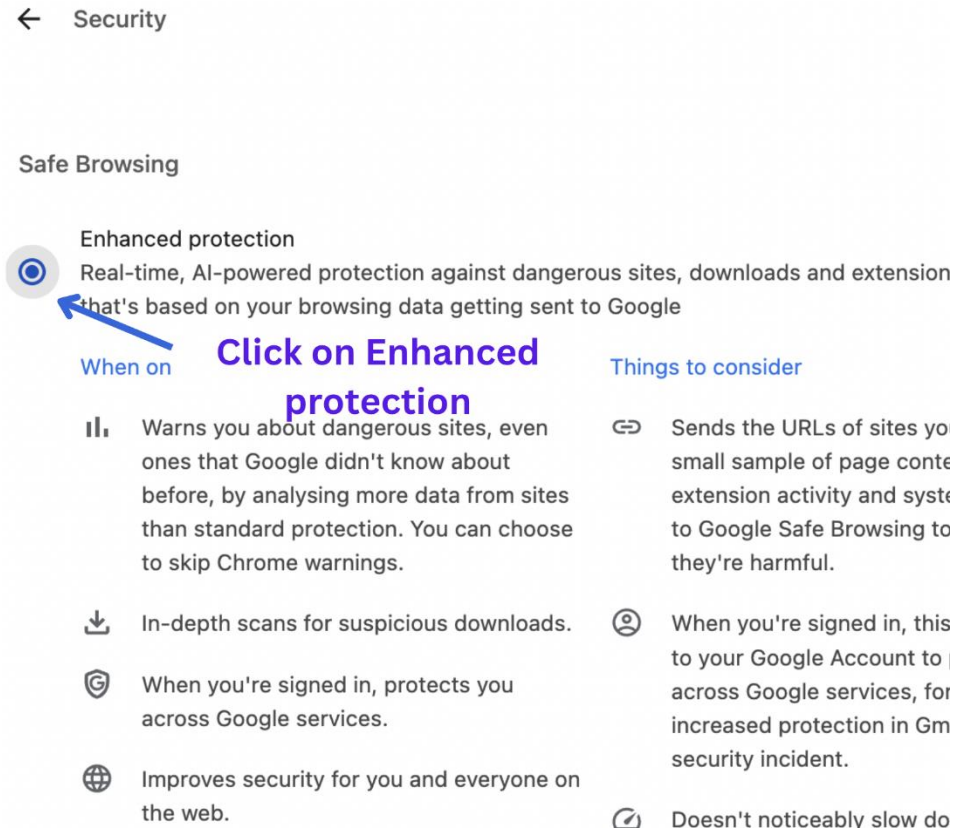


Figure 7.5 Accessing Chrome Browser Security for Safe Browsing

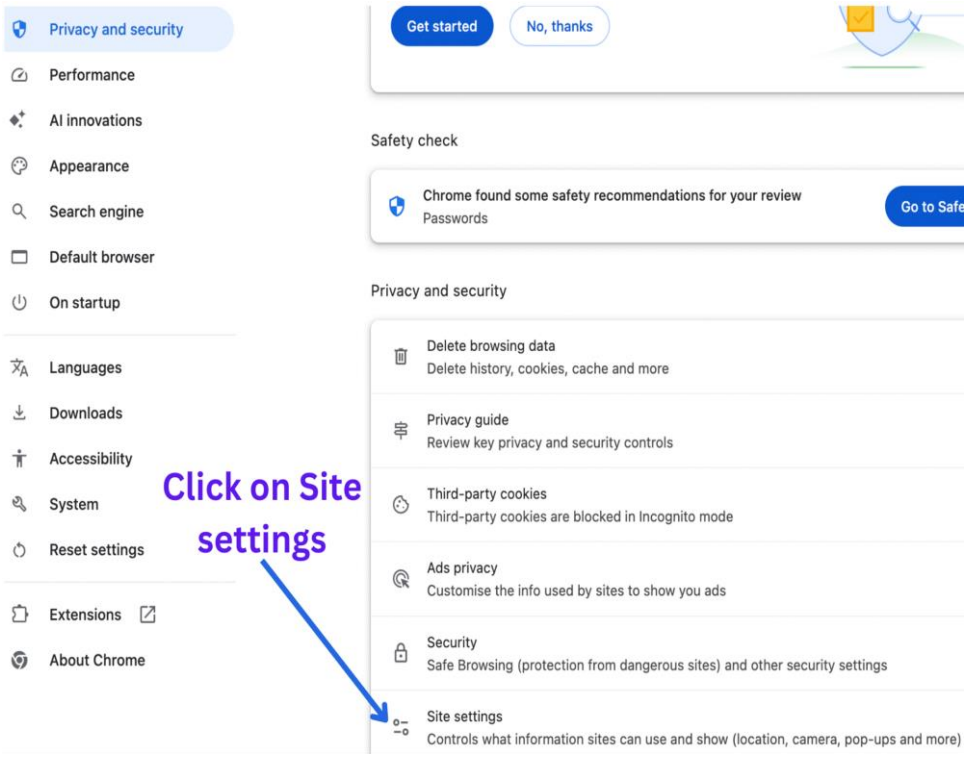


Figure 7.6 Accessing Chrome Browser Site settings option

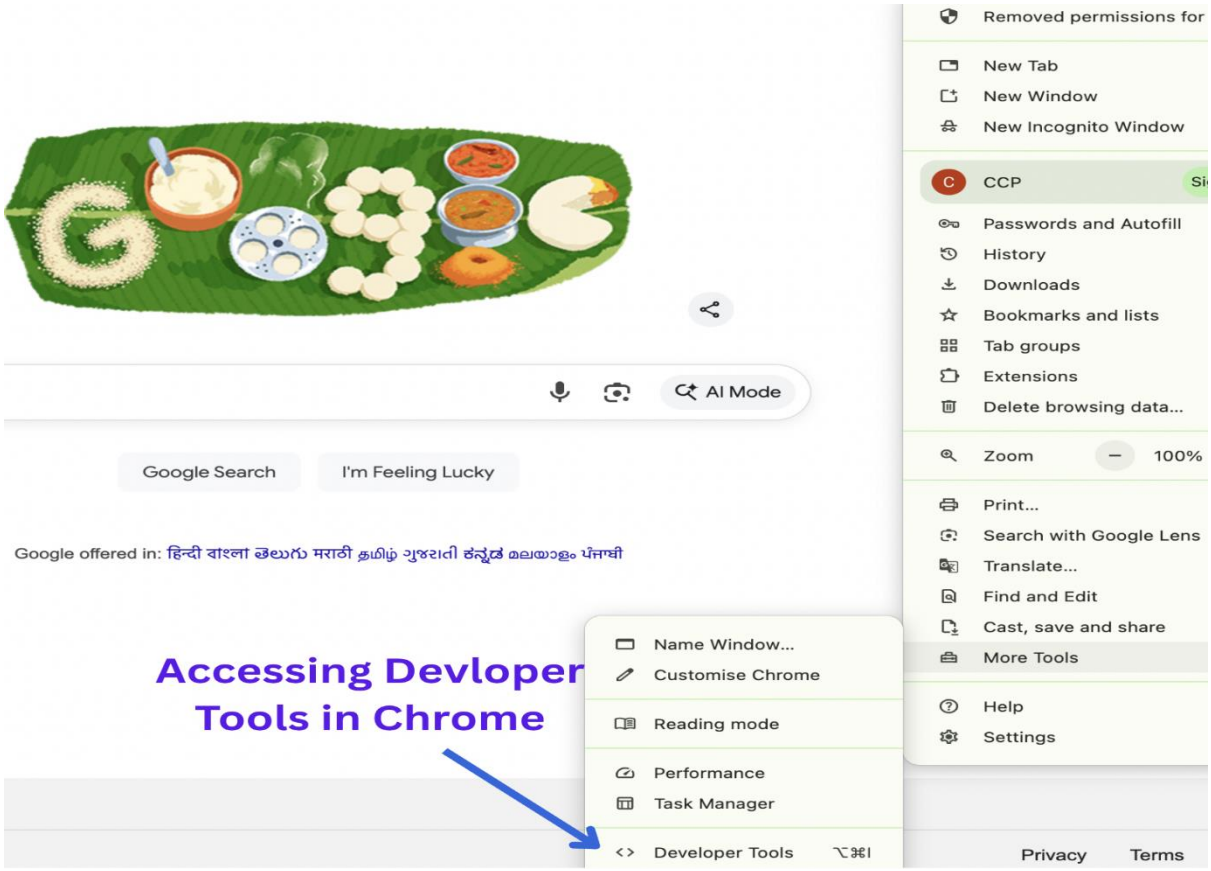


Figure 7.7 Accessing DevTools in Chrome Browser

1. Press **F12** or **Ctrl+Shift+I** to open DevTools (Figure 7.7).
2. Navigate to the **Application** tab:
    - Under **Storage** → **Cookies**, select a domain to view:
        - Name, Value
        - Secure, HttpOnly flags
        - Expiry date
3. Navigate to the **Network** tab:
    - Reload the page
    - Click on a request → View **Headers**:
        - **Request Headers**: User-Agent, Authorization, etc.
        - **Response Headers**: Set-Cookie, Content-Type, etc.

This inspection helps developers debug authentication flows and verify secure cookie handling.

Points to Remember:

- **Browser security** features, such as Content Security Policy(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.

7.8 Session Hijacking and Man-in-the-Middle (MITM) Attacks

Session Hijacking

Occurs when an attacker gains unauthorized access to a user's session. Methods include:

- **XSS (Cross-Site Scripting)**: Injecting malicious scripts to steal cookies.
- **Packet Sniffing**: Capturing unencrypted traffic on public networks.
- **Insecure Cookies**: Lack of Secure and HttpOnly flags.

MITM Attacks

Involve intercepting communication between the user and server. Attackers can:

- Read sensitive data
- Modify transactions
- Inject malicious content

These attacks are especially dangerous on public Wi-Fi or unsecured networks.

Prevention Strategies

- Enforce **HTTPS** with strong TLS configurations.
- Use **certificate pinning** to prevent spoofed certificates.
- Implement **multi-factor authentication (MFA)**.
- Educate users to avoid public Wi-Fi or use VPNs.

Practical Activity 7.1

Objective:

Learners will understand how to configure browser security settings in chrome & Firefox.

🛠 Tools & Platform Needed:

- Internet connection
- Laptop or desktop computer
- Web browser (Google Chrome, Mozilla Firefox)

Procedure:

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

Step 2. Assign each group a browser: Google Chrome or Mozilla Firefox.

Step 3. Each group will open their assigned browser.

Step 4. Access Browser Security Settings:

- For Chrome:
  - Go to Settings → Privacy and Security
  - Explore options like "Safe Browsing," "Site Settings," and "Security"
- For Firefox:
  - Go to Settings → Privacy & Security
  - Explore "Enhanced Tracking Protection," "HTTPS-Only Mode," and "Certificates"

Step 5. Configure Key Security Features:

- Enable Safe Browsing or Enhanced Tracking Protection
- Turn on HTTPS-Only Mode
- Manage Cookies and Site Permissions
- Review Certificate Authorities and Security Warnings

Step 6. Document Your Findings:

- Take screenshots of each security setting configured
- Note the purpose and impact of each setting on browser safety
- Discuss how these settings protect against phishing, malware, and insecure connections

Step 7. Present findings in class with slides showing configurations and their cybersecurity relevance.

Practical Activity 7.2

Objective: Learners will understand how WebSocket enables real-time communication between a client and server, and how to inspect WebSocket traffic using browser tools.

🛠 **Tools & Platform Needed:**

- Internet connection
- Laptop or desktop computer
- Web browser (Google Chrome, Mozilla Firefox)

Procedure:

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

Step 2. Each group will open a web browser (Chrome or Firefox).

Step 3. Visit the WebSocket demo site: https://echo.websocket.org/.ws

Step 4. Establish a WebSocket Connection:

- Use the demo interface to initiate a WebSocket connection
- Send a sample message (e.g., “Hello WebSocket”)
- Observe the echo response from the server

Step 5. Inspect WebSocket Communication:

- Open Developer Tools (F12 or Ctrl+Shift+I)
- Navigate to the Network tab
- Filter by WS (WebSocket)
- Click on the active WebSocket connection
- View message frames, request headers, and response data

Step 6. Document Your Findings:

- Describe the steps taken to initiate and inspect WebSocket communication
- Include screenshots of message frames and connection details
- Summarize how WebSocket differs from HTTPS and its role in real-time data exchange

- Discuss potential security concerns (e.g., lack of encryption, message interception)

Step 7. Present findings in class:

- Each group will prepare presentation slides showing the WebSocket process
- Explain the importance of secure WebSocket communication in modern web applications
- Suggest improvements or precautions for secure implementation

List of other suggested practical activities:

- Use Browser Developer Tools to inspect cookies and headers
- Explore HTTPS using SSL Lab
- Demonstration of MITM and Session Hijacking
- 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.)

- **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 application security is a multi-layered discipline that requires attention to architecture, protocols, user behavior, and threat mitigation. From understanding the roles of HTTP and HTTPS to inspecting cookies and headers using browser tools, every layer contributes to a secure digital experience.
- Tools like SSL Labs and Chrome DevTools empower users and developers to audit and improve their security posture.
- Meanwhile, awareness of threats like session hijacking and MITM attacks reinforces the need for encrypted communication and safe browsing habits. In today's connected world, cybersecurity isn't just a technical concern—it's a shared responsibility.
-

Topic	Key Takeaway
Web App Components	Frontend, backend, database, server, API
HTTP vs HTTPS	HTTPS encrypts data using SSL/TLS
SSL Labs	Tool to test HTTPS security
Secure Browsing	Use HTTPS, avoid suspicious links, enable safe browsing
Cookies & Sessions	Manage user state securely
Chrome Security Settings	Enable safe browsing, control site permissions
DevTools	Inspect cookies and headers
Session Hijacking & MITM	Encrypt data, secure sessions, avoid public Wi-Fi

ASSESSMENT

A. Multiple Choice Questions

1. What component of a web application handles user interface and interactions?
   a) Backend
   b) Web Server
   c) Frontend
   d) Database

2. Which protocol is used to securely transmit data between browser and server?
   a) HTTP
   b) FTP
   c) HTTPS
   d) SMTP

3. What does SSL/TLS provide in web communication?
   a) Faster page loading
   b) Encryption and authentication
   c) Server-side scripting
   d) Cookie storage

4. Which tool can be used to analyze a website's HTTPS configuration?
   a) Postman
   b) Wireshark
   c) SSL Labs
   d) GitHub

5. What browser feature helps detect phishing and malware websites? a) Incognito Mode
   b) Bookmark Manager
   c) Safe Browsing
   d) Developer Tools

6. What attribute should be set on cookies to prevent access via JavaScript?
   a) Secure
   b) HttpOnly

c) SameSite
d) Expires

7. Which Chrome DevTools tab allows inspection of cookies?
   a) Console
   b) Elements
   c) Application
   d) Sources

8. What is a common method used in session hijacking?
   a) Tokenization
   b) Cross-Site Scripting (XSS)
   c) HTTPS
   d) Firewall

9. What does a Man-in-the-Middle (MITM) attack target?
   a) Database schema
   b) Data transmission
   c) User interface
   d) Data storage

10. Which protocol has been deprecated and replaced by TLS?
    a) HTTP
    b) SSL
    c) FTP
    d) SMTP

B. Fill in the Blanks

1. _____ is the protocol used to transmit data securely between browser and server.
2. The _____ component of a web application handles business logic and database queries.
3. SSL and TLS provide _____ and authentication for web communication.
4. _____ Labs is a tool used to evaluate HTTPS security configurations.
5. Cookies should be set with the _____ flag to prevent access via JavaScript.
6. Chrome's _____ tab allows users to inspect cookies and local storage.
7. A _____ attack involves intercepting communication between client and server.
8. Session hijacking often uses _____ to steal session tokens.
9. The _____ attribute on cookies helps prevent cross-site request forgery.
10. Secure browsing practices include enabling _____ protection in browser settings.

C. True or False

1. HTTPS encrypts data during transmission.
2. SSL is more secure than TLS.
3. Cookies can store session IDs.
4. Chrome DevTools cannot inspect cookies.

5. Safe Browsing helps detect phishing websites.
6. Session hijacking is harmless and rarely used.
7. HttpOnly cookies are accessible via JavaScript.
8. MITM attacks target data storage.
9. SSL Labs can be used to test TLS configurations.
10. Using public Wi-Fi without a VPN is safe for online banking.

D. Short Answer Questions

1. What are the main components of a web application?
2. How does HTTPS differ from HTTP in terms of security?
3. What is the purpose of the HttpOnly flag in cookies?
4. Name two tools used to inspect web security configurations.
5. What is session hijacking and how can it be prevented?

E. Long Answer Questions

1. Explain the architecture of a web application, detailing the roles of frontend, backend, database, and web server.
2. Describe the importance of HTTPS and SSL/TLS in securing web communication. How can tools like SSL Labs help evaluate a website's security?
3. Discuss session management and cookie security. How do browser tools and secure attributes help prevent attacks like session hijacking and MITM?

ANSWER KEY

A. Multiple Choice Questions

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

B. Fill in the Blanks

1.HTTPS, 2.Backend, 3.encryption, 4.SSL, 5.HttpOnly, 6.Application, 7.Man-in-the-Middle, 8.Cross-Site Scripting (XSS), 9.SameSite, 10.Safe Browsing

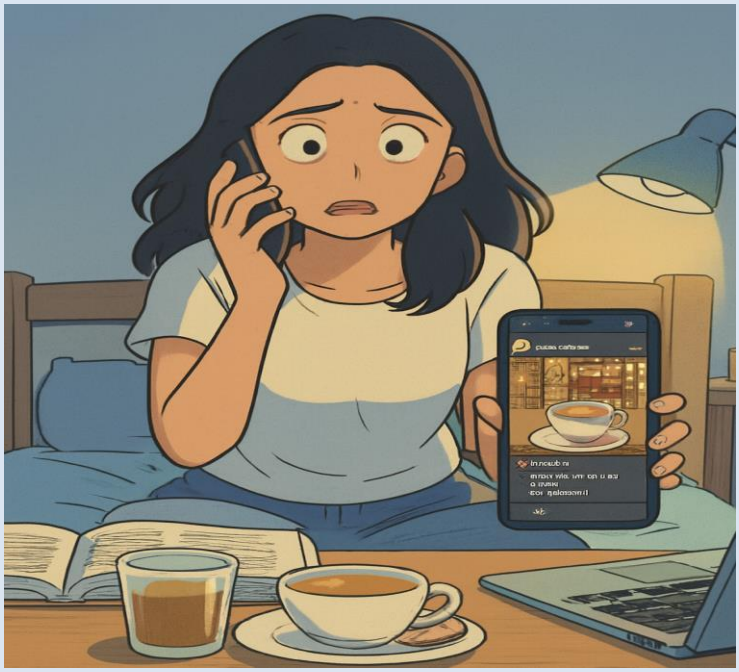
C. True or False

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

Chapter-8

Social Media and its Security

Jyoti was a college student in Pune. She loved posting pictures and updates on Instagram—her weekend trips to Lonavala, chai breaks at cute cafés, and fun moments with friends at college. One Saturday evening, she uploaded a photo from a cozy café in Koregaon Park with the caption, "New favourite chai spot! #ChaiVibes." She tagged the café location, thinking it was harmless. Two days later, she got a call from an unknown number. The voice on the other side was calm but strange. "Hi Jyoti, You really like Chai Vibes café, don't you? You're studying computer science, right? Are you in your hostel now?" Jyoti was shocked. How did this person know so much about her? She quickly checked her Instagram settings. Everything was public—her location, college name, daily routine, even her class timings. The person had been following her posts and learning about her life. Scared, Jyoti changed her privacy settings, removed personal details, and stopped tagging locations. That day taught her a big lesson: sharing too much online can be risky.



From then on, Jyoti became more careful about what she posted and who could see it. She understood the importance of social media safety. Just like Jyoti, we all need to think before we share. It's important to check our privacy settings, avoid posting sensitive details, and stay alert—because not everyone online has good intentions.

In this chapter, we will explore types of social media, their advantages and disadvantages, security issues, and ways to enhance privacy and security, the configuration of privacy settings on Facebook and Instagram, identify common threats such as phishing and impersonation, and provide practical strategies for reporting and blocking malicious actors. It also includes classroom activities and demos to reinforce learning.

8.1 Introduction to Social Media

Figure 8.1 The world of social media

Social media platforms like Facebook and Instagram have revolutionized how people connect, share, and express themselves. From personal updates to professional branding, these platforms offer immense value. However, with this connectivity comes vulnerability. Users are exposed to privacy breaches, scams, impersonation, and phishing attacks. For educators and learners alike, understanding how to safeguard personal information and recognize threats is essential in today's digital landscape (*Figure 8.1).*

Here are some of the main types of social media:

8.1.1 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

Figure 8.2 Facebook Logo

- **Microblogging Platforms:** These are platforms that 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

Figure 8.3 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

Figure 8.4 Logo of Instagram, Snapchat and Youtube

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

  Examples: WhatsApp, Telegram, Messenger.

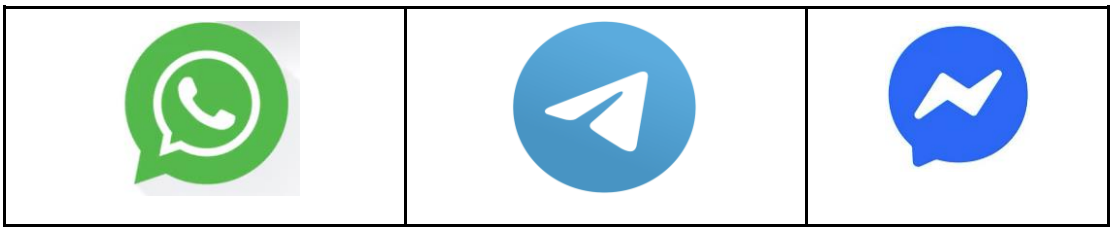


Figure 8.5 Logo of WhatsApp, Telegram & Messenger

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

  Examples: LinkedIn, Xing

Figure 8.6 Logo of LinkedIn and Xing

8.1.2 Advantages Of Social Media

Social media platforms have transformed communication, education, and commerce. Their benefits include:

- **Global Connectivity:** Users can connect with friends, family, and professionals across borders.
- **Information Sharing:** Real-time updates on news, trends, and educational content.
- **Business and Marketing:** Entrepreneurs and brands use platforms for promotion and customer engagement.
- **Community Building:** Groups and forums foster shared interests and support networks.
- **Learning Opportunities:** Tutorials, webinars, and educational pages make learning accessible.

For students and educators, social media can be a collaborative space for sharing ideas, showcasing projects, and accessing global resources.

Figure 8.7 Privacy concerns of all types of social media

8.1.3 Disadvantages of Social Media

Despite its benefits, social media poses several challenges:

- **Privacy Risks:** Oversharing can expose users to identity theft or stalking.
- **Cyberbullying:** Harassment and trolling are common, especially among youth.
- **Misinformation:** Fake news and manipulated content spread rapidly.
- **Mental Health Impact:** Excessive use may lead to anxiety, depression, or low self-esteem.
- **Addiction and Distraction:** Constant notifications and scrolling reduce productivity.

Educators should help learners critically evaluate content and manage screen time.

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).
  - 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.

8.1.4 Security Issues and Challenges While Using Social Media

Social media platforms are vulnerable to various security threats:

- Phishing Attacks: Fake messages or links trick users into revealing credentials.
- Impersonation and Fake Profiles: Scammers create fake accounts to deceive or defraud.
- Data Breaches: Personal data may be leaked or sold without consent.
- Malware and Spyware: Clicking on malicious links can infect devices.
- Encrypted Messaging Risks: While offering privacy, these services can also shield criminal activity.

Security awareness is essential for safe participation in digital communities.

8.1.5 Tips to safe and secure use of Social Media

To stay protected, users should adopt smart habits and settings:

- **Use Strong Passwords:** Combine letters, numbers, and symbols. Avoid using the same password across platforms.
- **Enable Two-Factor Authentication (2FA):** Adds an extra layer of security.
- Review Privacy Settings Regularly: Limit who can see your posts, stories, and personal info.
- **Be Cautious with Links and Attachments:** Verify sources before clicking.
- **Avoid Oversharing:** Don't post sensitive details like location, ID numbers, or financial info.
- **Report Suspicious Activity:** Use platform tools to report and block threats.
- **Educate Yourself and Others:** Stay updated on scams and security practices

8.2 Configuring Privacy Settings on Social Media

8.2.1 Facebook: Building a Secure Profile

Facebook offers granular privacy controls that allow users to manage who sees their content, interacts with them, and accesses their personal information. To begin, users should navigate to Settings & Privacy > Settings > Privacy.

Key settings include:

- **Who can see your future posts:** Set this to Friends or Only Me to limit exposure.
- **Limit past posts:** This retroactively restricts visibility of older content.
- **Who can send you friend requests:** Choosing Friends of Friends reduces unsolicited requests.
- **Profile and tagging settings:** Enable review of tags before they appear on your timeline and restrict who can tag you.

These settings help users maintain control over their digital footprint and reduce the risk of unwanted attention or data harvesting.

On facebook platform navigate to Settings & Privacy enable, review, manage and control

above options one by one:

- ➔ Review Privacy Settings:
  - ◆ Go to Settings & Privacy > Privacy Checkup.
  - ◆ Review and control who can see your posts, profile information, and manage your block list*(Figure 8.8)*.
- ➔ 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*(Figure 8.9)*.

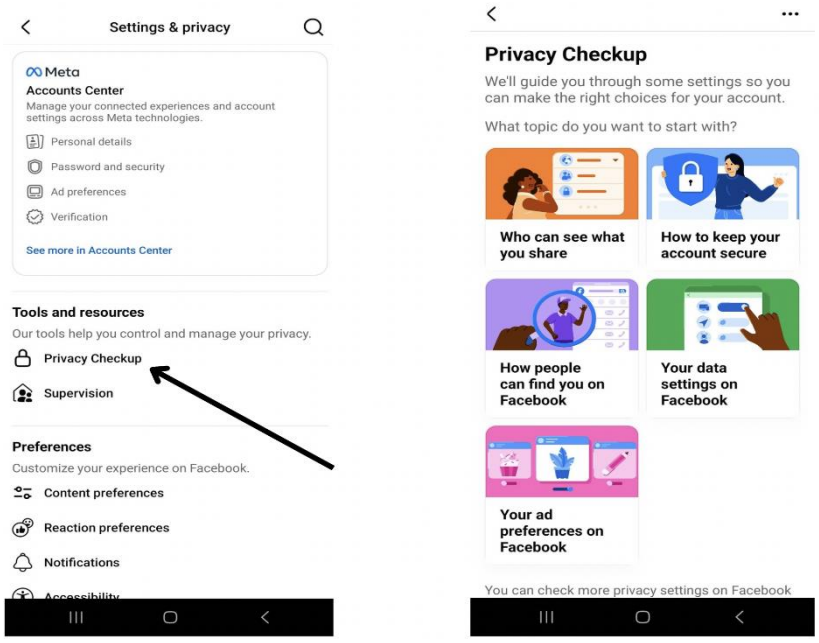


Figure 8.8 Privacy Checkup in Facebook App

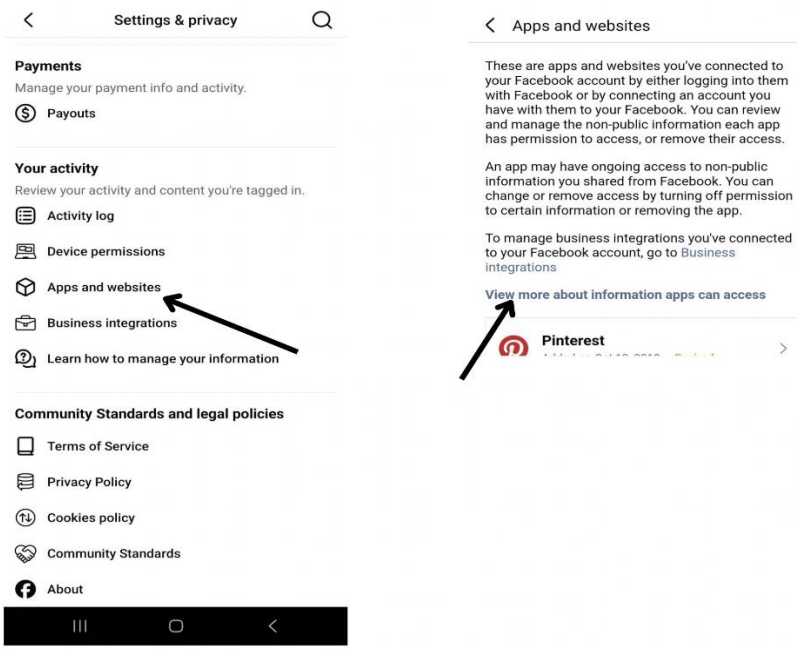


Figure 8.9 Managing other apps permissions in Facebook App

8.2.2 Instagram: Privacy in a Visual World

Instagram's visual nature makes it a prime target for impersonation and scams. Users should start by accessing Profile > Menu (☰) > Settings and Privacy.

Recommended settings:

- **Private Account:** Only approved followers can view posts and stories.
- **Story Controls:** Hide stories from specific users and restrict message replies.
- **Activity Status:** Disable this to prevent others from seeing when you're online.
- **Blocked Accounts:** Regularly review and block suspicious profiles.

These settings empower users to curate their audience and minimize exposure to threats. On instagram platform navigate to Settings and enable, review, manage and control above options one by one:

➔ Make Your Account Private:

- Go to Settings and activity>Account Privacy.
- Toggle on "Private Account" to limit who can see your posts. (*Figure 8.10)*
- Use the Blocked Accounts feature to prevent unwanted interactions.
- Limit app permissions and monitor third-party app access. (*Figure 8.11)*

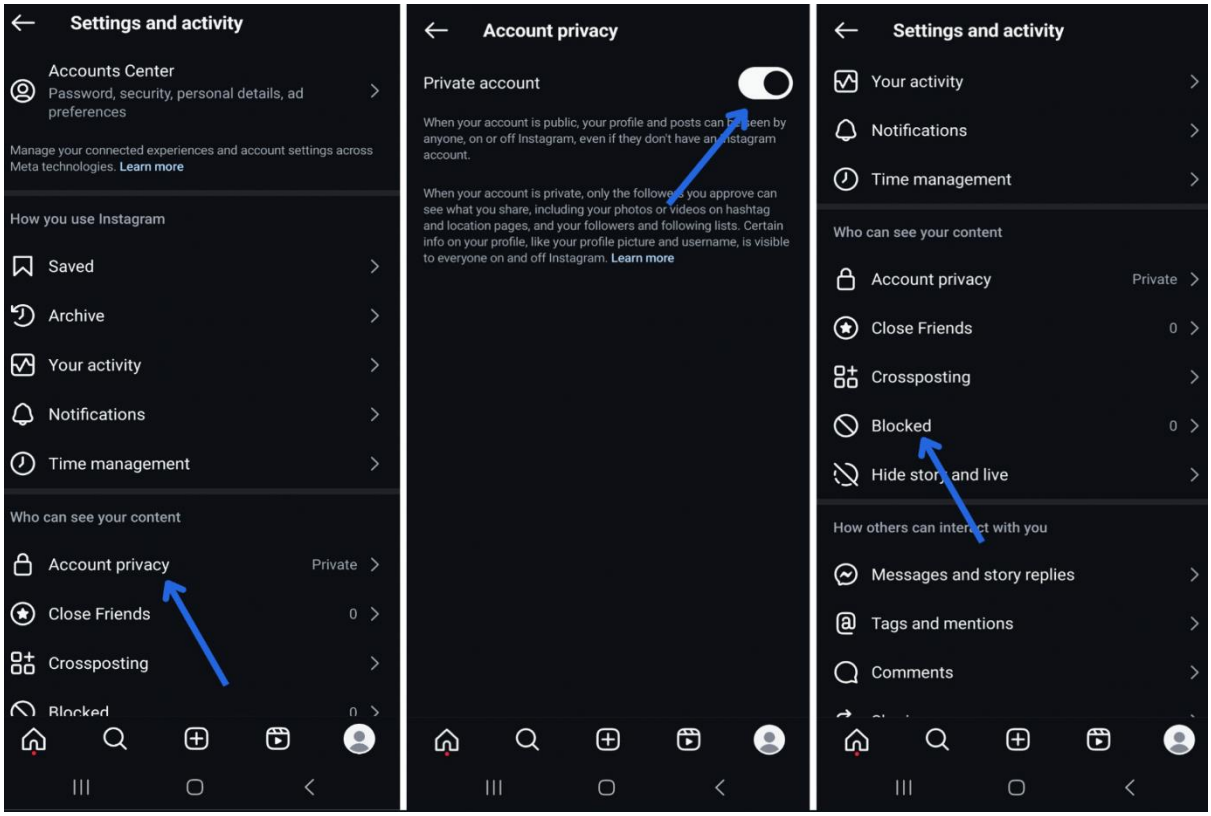


Figure 8.10 Making Instagram account as private and accessing Blocked feature

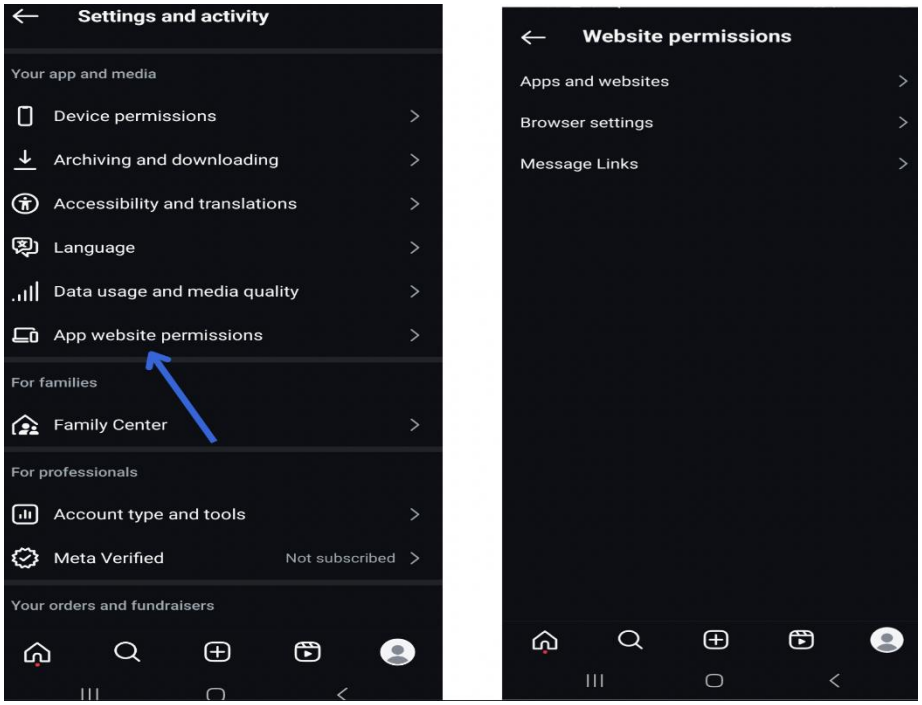


Figure 8.11 App website permissions while using Instagram app

➔ Review Account Activity:

- Go to Settings and activity>

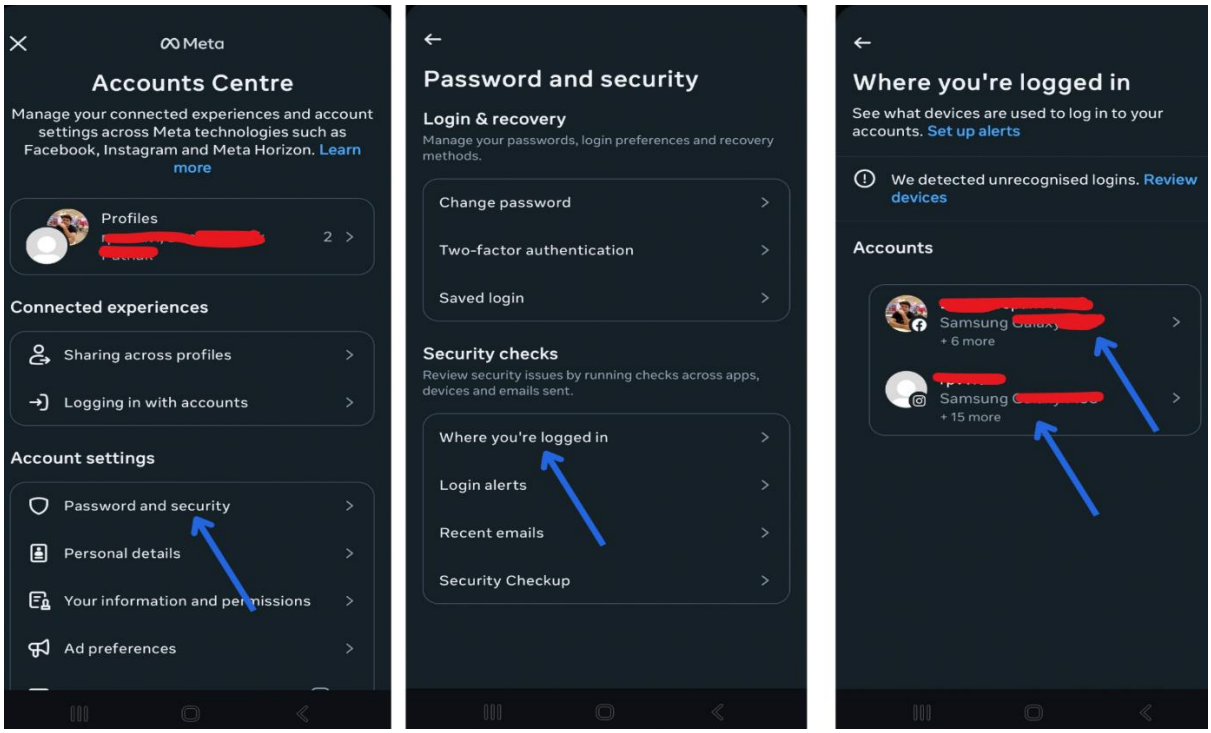


Figure 8.12 Review account activity in Instagram app

- Tap Accounts Center
- Tap Password and security
- Tap Where you're logged in
- Review and log out of any suspicious devices or locations.(*Figure 8.12)*

➔ Manage Comment Controls:

- Go to Settings and activity >Comments.
- Filter out offensive comments and block specific users from commenting on your posts (*Figure 8.13)*.

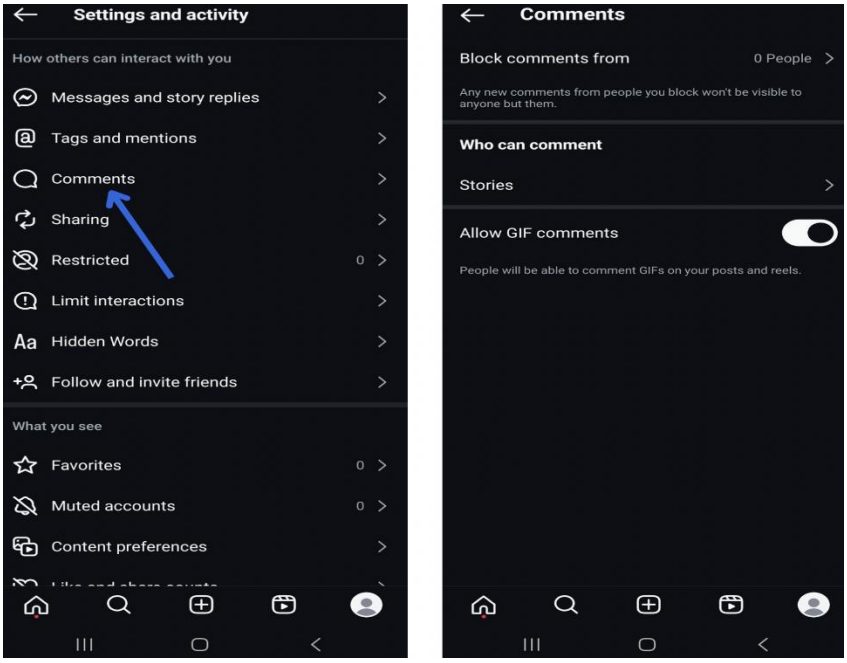


Figure 8.13 Manage comment control in Instagram app

➔ Manage Tags and mentions:

- Go to Settings and activity >Tags and mentions.
- Allow and Don't allow tags and mentions (*Figure 8.14)*

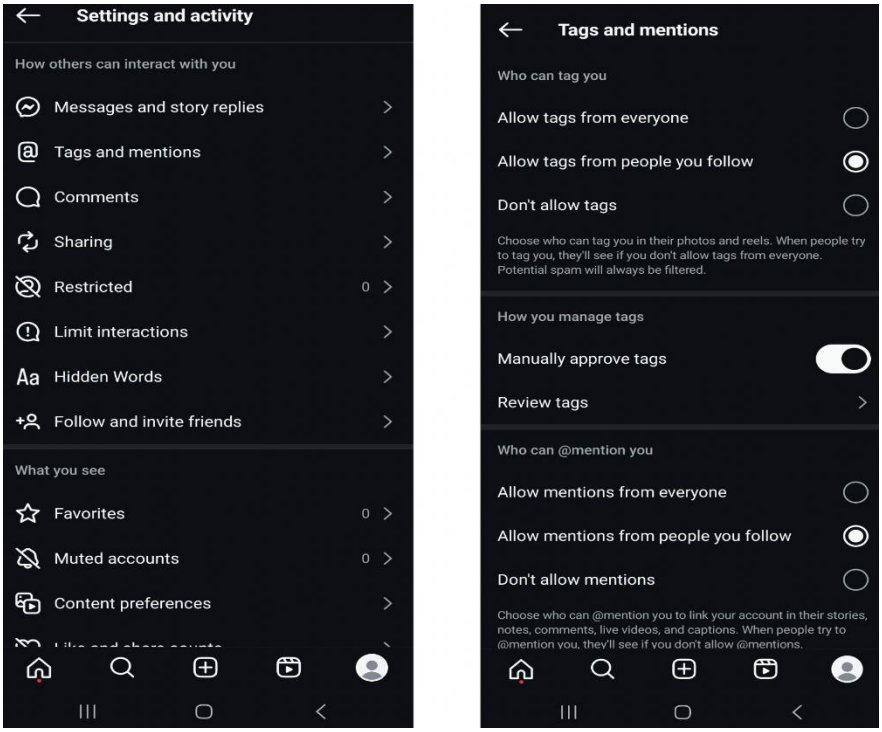


Figure 8.14 Manage Tags and mentions in Instagram app

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.

8.3 Recognizing Phishing, Fake DMs, and Emails

8.3.1 Phishing: The Art of Deception

Phishing is a deceptive tactic used to trick users into revealing sensitive information. It often involves emails or messages that appear to be from trusted sources but contain malicious links or requests.

Common signs of phishing include:

- Urgent language (e.g., "Your account will be suspended!").
- URLs that mimic official domains (e.g., www.faceboook.com).
- Requests for passwords, OTPs, or financial details.

Educators should emphasize skepticism and verification. Encourage learners to hover over links before clicking and to verify sender details.

8.3.2 Fake DMs and Emails: The Digital Impostors

Direct messages (DMs) and emails are frequently used to impersonate brands, influencers, or friends. These messages may offer fake giveaways, job offers, or emotional appeals for money.

Red flags include:

- Generic greetings like "Dear user".
- Poor grammar and spelling.
- Suspicious attachments or shortened links.

Classroom Tip: Use anonymized examples of phishing emails and DMs to help students practice identifying threats.

8.4 Impersonation and Fake Profiles

Anatomy of a Fake Profile

Fake profiles are created to deceive, scam, or impersonate real individuals. They often have minimal content, generic profile pictures, and vague bios.

Indicators of fake profiles:

- Recently created accounts with few followers.
- Stock images or celebrity photos as profile pictures.
- Inconsistent or overly flattering bios.

8.5 Social Media Scams and How to Avoid Them

8.5.1 Common Scams

Social media scams come in many forms, including:

- Romance scams: Fake relationships used to extract money.
- Investment scams: Promises of high returns with fake endorsements.
- Giveaway scams: "You've won!" messages asking for personal info.
- Job scams: Fake recruiters requesting fees or documents.

These scams exploit trust and urgency. Victims often feel embarrassed, making reporting less likely.

8.5.2 Prevention Strategies

- Never share OTPs or passwords.
- Avoid clicking on unknown links.
- Use two-factor authentication (2FA).
- Verify profiles before engaging.

Educators should encourage open discussions and normalize reporting suspicious activity.

8.6 Reporting and Blocking Threats

Facebook: Taking Action

To report a threat:

- Go to the profile or post.
- Click More (···) > Report.
- Select the reason (e.g., harassment, impersonation).

To block:

- Navigate to Settings > Blocking > Add to Block List.

Instagram: Defending Your Space

To report:

- Visit the profile or message.
- Tap More (···) > Report.
- Choose the appropriate category.

To block:

- Tap Block from the same menu.

Practical Activity 8.1: Fake Profile Detection

Objective: Train students to identify fake profiles.

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

Group Formation and Task Assignment:

1. Present three anonymized profiles (one real, two fake).
2. Ask students to analyze:
    - Profile picture authenticity.
    - Post history and engagement.
    - Language and tone in bios.
3. Facilitate a discussion on red flags and vote on which profiles are fake.

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 class and discuss the importance of Social media security.

This activity builds critical thinking and digital literacy.

Practical Activity 8.2:

Objective: Learners will conduct Reporting Simulation

Scenario: A student receives a suspicious DM offering money.

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

Group Formation and Task Assignment:

1. In groups, students analyze the message.
2. Decide whether it's a threat.
3. Demonstrate how to report and block the sender.

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 class and discuss the importance of Social media security.

This simulation reinforces practical skills and builds confidence.

List of other suggested practical activities:

- **Instagram Account Protection:** Learners will configure Privacy and Security Settings on Instagram to protect personal information.
- **Facebook Account Protection:** Learners will configure Privacy and Security Settings in facebook to protect personal information.
- **Whatsapp Account Protection:** Learners will configure Privacy and Security Settings in Whatsapp to protect personal information.
- **Enabling Two-Factor Authentication (2FA):** To implement two-factor authentication for enhanced security on a social media platform.

Summary

- This chapter explores the dual nature of social media—its power to connect and educate, and its potential to expose users to privacy and security risks. Platforms like Facebook, Instagram, and X offer tools to manage visibility, control interactions, and protect personal data. Users are encouraged to configure privacy settings such as limiting post visibility, enabling two-factor authentication, and setting accounts to private.
- The chapter highlights common threats including phishing, impersonation, fake profiles, and scams like romance or investment fraud. It explains how to identify suspicious messages and profiles, and how to report and block malicious users. Security challenges such as data breaches, malware, and misinformation are discussed, along with their impact on mental health and digital safety.
- To mitigate these risks, the chapter provides practical tips: use strong passwords, avoid oversharing, verify links, and regularly review account activity. It also outlines the advantages (global connectivity, learning, marketing) and disadvantages (privacy concerns, cyberbullying, addiction) of social media.
- Interactive classroom activities—like fake profile detection demos and reporting simulations—are included to reinforce learning and empower students to become responsible digital citizens.

ASSESSMENT

A. Multiple Choice Questions

1. What is the primary purpose of enabling two-factor authentication (2FA)?
   a) To increase post visibility
   b) To prevent account deletion
   c) To add an extra layer of security
   d) To allow anonymous browsing

2. Which of the following is a sign of a phishing message?
   a) Personalized greeting
   b) Verified sender address
   c) Urgent request for personal info
   d) Secure HTTPS link

3. On Instagram, what does switching to a private account do?
   a) Deletes all followers
   b) Allows only approved followers to view content
   c) Blocks all messages
   d) Hides your account from search

4. Which of the following is NOT a common social media scam?
   a) Romance scam
   b) Investment scam
   c) Weather forecast scam
   d) Job scam

5. What is the best way to detect a fake profile?
   a) Check for verified badge
   b) Look for high-quality images
   c) Analyze post history and engagement
   d) Count the number of followers

6. Which Facebook setting limits who can tag you in posts?
   a) Timeline review
   b) Activity log
   c) Story controls
   d) Tagging permissions

7. What is a disadvantage of social media?
   a) Real-time updates
   b) Global connectivity
   c) Cyberbullying
   d) Business promotion

8. Which of the following is a security issue on social media?
   a) Sharing memes
   b) Using hashtags
   c) Data breaches
   d) Posting travel photos

9. What should you do if you receive a suspicious DM?
   a) Reply politely
   b) Share it with friends
   c) Report and block the sender
   d) Ignore and delete

10. Which feature helps you control who sees your Facebook posts?
    a) News Feed
    b) Privacy Settings
    c) Messenger
    d) Notifications

B. Fill in the Blanks

1. _____ is a technique used to trick users into revealing sensitive information through fake messages.
2. On Instagram, the _____ account setting restricts content visibility to approved followers.
3. _____ authentication adds a second layer of security to your login process.
4. A fake profile often uses _____ images and has limited post history.
5. Cyberbullying is a major _____ of social media.
6. Facebook's _____ settings allow users to control who can tag them in posts.
7. Sharing personal details like your home address online can lead to _____ risks.
8. A _____ scam involves fake romantic relationships to extract money.
9. Clicking on unknown links may result in _____ infections.
10. Reporting and _____ are key actions to take against online threats.

C. True or False

1. Malware can be spread through social media links.
2. Social media platforms are completely safe if you use strong passwords.
3. Instagram allows users to hide their activity status.
4. Phishing messages often come from verified sources.
5. Facebook allows users to limit who can send them friend requests.
6. Fake profiles usually have detailed bios and frequent posts.
7. Two-factor authentication makes it harder for hackers to access your account.
8. Cyberbullying is a rare issue on social media.
9. Reporting a scammer on Instagram automatically deletes their account.
10. Social media can be used for educational purposes.

D. Short Answer Questions

1. What are three signs of a phishing message?
2. How can users detect a fake social media profile?
3. What is the role of privacy settings on Facebook?
4. Name two common types of social media scams.
5. Why is it important to report and block suspicious accounts?

E. 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

A. Multiple Choice Questions

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

B. Fill in the Blanks

1. Phishing, 2. Private, 3. Two-factor, 4. stolen, 5. disadvantage, 6. Tagging, 7. security, 8. romance, 9. malware, 10. Blocking

C. True or False

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

Chapter-9

Digital Payments and Banking Fraud

Arjun was a hardworking student who dreamed of buying a gaming laptop. To earn money, he started doing small freelance jobs online. One evening, he saw an ad: "Premium Gaming Laptop for ₹30,000! Limited Time Offer!" The website looked real, with good reviews. Excited, Arjun quickly paid for it.

Days passed, but the laptop never came. He realized he had been scammed. Upset but hopeful, Arjun asked his elder brother Ravi, a cybersecurity expert, for help. They contacted the cybercrime cell and shared all details. With Ravi's help, the scammer was found and Arjun got his money back.

This experience taught Arjun to be careful online. He learned to check websites for safety signs like "https" and avoid deals that look too good. Later, he bought his dream laptop and started telling others about online safety, turning his mistake into a lesson for everyone.

9.1 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.

Digital payment systems refer to the electronic transfer of money or digital currency using internet-enabled platforms. These systems have transformed the financial landscape by offering:

- Speed: Instant transactions across geographies.
- Convenience: No need for physical cash or cheques.
- Security: Encrypted and authenticated processes.

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 (*Figure 9.1).*

Figure 9.1 Unified Payment System (UPI)

9.1.1 Digital Payment Steps

Step 1: Initiate Payment First, You decide to make a purchase or send money digitally. This usually happens on your smartphone, where you tap a "Pay Now" or "Send Money" button within an app like a mobile wallet, banking app, or a merchant's e-commerce app.

Step 2: Sender's Bank (or Payment Source) Once you initiate the payment, your chosen payment method (e.g., your bank account linked to UPI, a debit/credit card, or a digital wallet) is accessed. Your bank or the payment provider (like a wallet company) verifies that you have sufficient funds or credit for the transaction.

Step 3: Enter Details & Authenticate At this stage, you typically enter necessary details. If you're buying something, it might be selecting the item. If sending money, it's the recipient's details (e.g., UPI ID, bank account number). Crucially, you then authenticate the transaction. This could be by entering your PIN, a one-time password (OTP) sent to your phone, or using biometrics like a fingerprint or face scan. This step is vital for security.

Step 4: Payment Gateway / Network After authentication, your payment request travels through a secure "payment gateway" or network. Think of this as the digital bridge that connects your bank to the recipient's bank. These gateways are secure platforms (like UPI, Visa, Mastercard, RuPay) that process and encrypt the transaction information, ensuring it's safe from prying eyes.

Step 5: Receiver's Bank Next, the payment gateway communicates with the recipient's bank. It sends the encrypted transaction details, requesting that the funds be credited to the recipient's account.

Step 6: Confirm Payment Once the transaction is processed and approved by both banks (or payment providers), the funds are transferred. You'll usually see a "Payment Successful" message on your screen. This confirms that your money has left your account and is on its way.

Step 7: Receive Confirmation Message Finally, both you and the recipient will receive a confirmation message. This might be an SMS, an email, or a notification within the app, stating that the transaction was successful, along with details like the amount, date, and transaction ID. This serves as a digital receipt.

Throughout this entire process, advanced encryption and security protocols are at play to ensure that your financial information is protected, making digital transactions both convenient and safe.

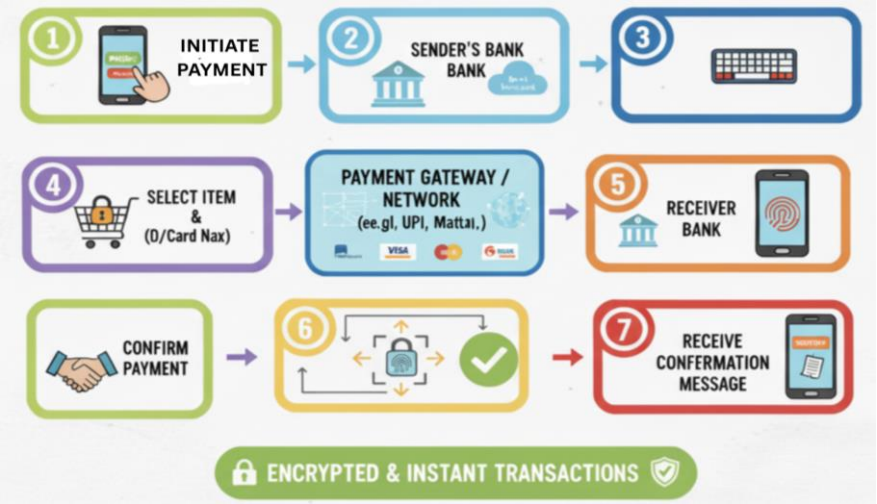


Figure 9.2: How does the Digital Payment System Work?

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

9.2 Types of Digital Payment Methods

1. Mobile Wallets

Mobile wallets store prepaid money digitally and allow transactions without needing a bank account. They support:

- Peer-to-peer transfers
- Merchant payments
- Utility bill payments
- Online shopping

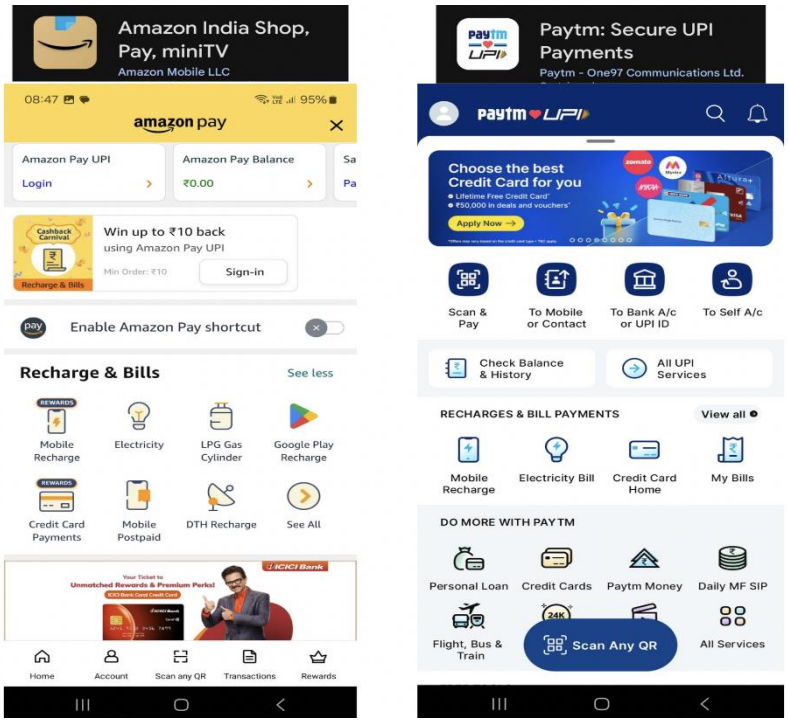


Figure 9.3 Amazon Pay and Paytm apps

Popular Indian Mobile Wallets

Wallet	UPI Required	Key Features
Paytm Wallet	No	Wallet-to-wallet transfers, bill payments
PhonePe	Optional	UPI + wallet option
Amazon Pay	No	Prepaid wallet for purchases
MobiKwik	No	Recharge, transfers
Freecharge	No	Utility payments, shopping
JioMoney	No	Recharges, shopping
Airtel Thanks	No	Bill payments, money transfers
PayZapp	No	Direct payments via wallet

International Mobile Wallets

- Apple Pay, Samsung Pay: NFC-based contactless payments
- Google Pay (GPay): Wallet + UPI hybrid

Figure 9.4 Airtel Thanks and PayZapp

2. Credit/Debit Card Payments

Cards issued by Visa, MasterCard, and RuPay are used for:

- POS transactions
- Online shopping
- Bill payments

Figure 9.5 Debit/Credit Card

Globally accepted, they offer fraud protection and reward programs.

3. Bank Transfers

Direct transfers between bank accounts using:

- India:
  - NEFT: Settles in batches
  - RTGS: Real-time for large amounts
  - IMPS: Instant 24/7 transfers
- International:
  - SWIFT: Global interbank messaging
  - SEPA: Eurozone transfers

4. Unified Payments Interface (UPI)

UPI allows real-time interbank transactions via mobile apps. Features include:

- Peer-to-peer transfers
- Merchant payments
- Bill payments

Popular UPI apps: BHIM, PhonePe, Google Pay

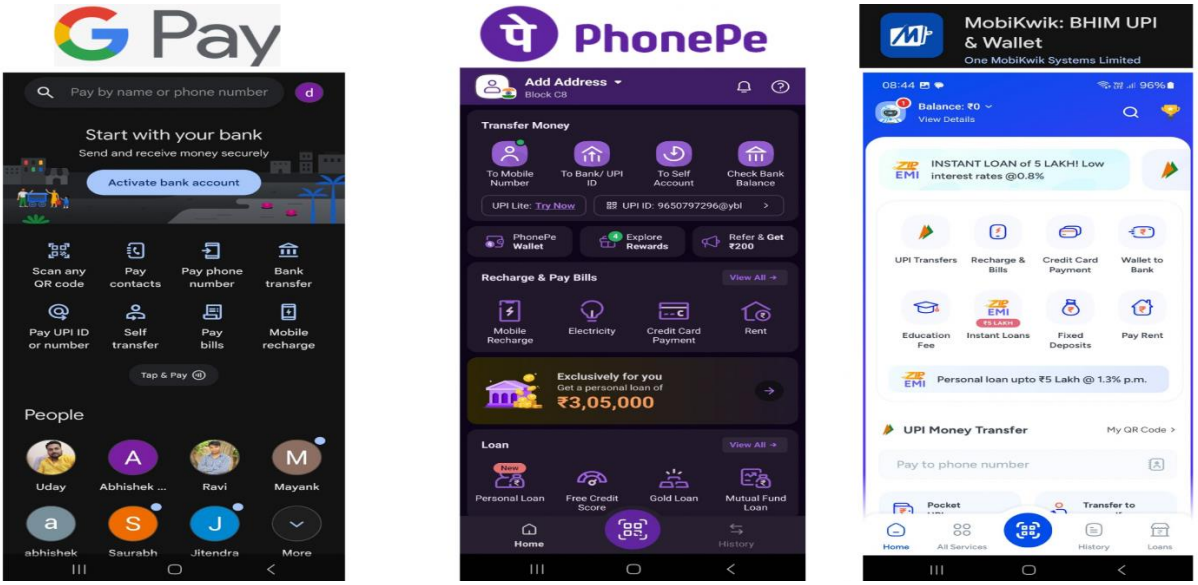


Figure 9.6 G Pay, Phonepay and MobiKwik apps

5. QR Code Payments

QR stands for quick response. QR codes enable quick scanning for payments. Widely used by:

- Street vendors
- Small businesses
- E-commerce platforms

Examples:

- India: Bharat QR, Paytm QR, PhonePay QR
- China: Alipay, WeChat Pay

Figure 9.7 Phonepay QR Code

6. Cryptocurrency Payments

Digital currencies like Bitcoin and Ethereum offer decentralized transactions. Used for:

- Online purchases
- Investments
- Remittances

Indian platforms: CoinDCX, WazirX

Global platforms: Coinbase, Binance

Note: Cryptocurrency Payments are subjected to regulatory scrutiny due to volatility and anonymity.

7.Contactless Payments

NFC-enabled cards and devices allow tap-and-pay transactions. Used for:

- Retail purchases
- Public transport

Examples:

- Apple Pay, Samsung Pay
- Bharat QR (India)

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).

9.3 Security Issues in Digital Payments

Despite their benefits, digital payments face several threats:

1. Phishing Attacks

Fake emails or websites trick users into revealing credentials.

Example: A user receives a fake Paytm email asking to "verify account."

2. Malware & Ransomware

Malicious software steals data or locks devices.

Example: A ransomware encrypts files and demands payment.

3. Man-in-the-Middle (MitM) Attacks

Hackers intercept data during transmission.

Example: Intercepting login credentials over public Wi-Fi.

4.Data Breaches

Hackers access stored user data from payment platforms.

Example: A breach at a payment gateway exposes credit card info.

5.Social Engineering

Manipulating users into revealing confidential info.

Example: A caller pretends to be bank IT support and asks for passwords.

9.3.1 Techniques to Address Digital Payment Security

Technical Measures

- Multi-Factor Authentication (MFA): Password + OTP + biometrics
- Encryption: SSL/TLS for secure data transmission
- Tokenization: Replace sensitive data with encrypted tokens

Operational Measures

- Security Audits: Regular penetration testing
- Fraud Detection Systems: AI-based anomaly detection
- Data Minimization: Store only essential user data

Awareness & Regulation

- User Education: Campaigns on phishing and safe practices
- Regulatory Frameworks: GDPR (EU), IT Act (India)

9.4 Digital and Online Banking Frauds

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.

Common Types

Fraud Type	Description	Cause
Phishing/Smishing	Fake emails/SMS	Poor filtering, user unawareness
Vishing	Fake calls from “bank”	Social engineering

Malware/Ransomware	Infects devices	Unsafe downloads
SIM Swap	Duplicate SIM to access OTPs	Weak telecom protocols
Account Takeover	Unauthorized access	Weak passwords
E-wallet/UPI Fraud	Unauthorized transactions	Sharing OTPs
Card Skimming	Cloning via POS/ATM	Outdated tech
Fake Banking Apps	Mimic real apps	Unverified sources
MITM Attacks	Intercept communication	Public Wi-Fi
Identity Theft	Use of stolen data	Phishing, hacking
Cheque Fraud	Forged cheques	Signature tampering
Loan Fraud	Fake documents	Misrepresentation
Money Laundering	Concealing illicit funds	Shell accounts
Insider Fraud	Bank employee misconduct	Lack of controls

9.5 Mitigation Strategies for online Banking Frauds

For Banks

- Cybersecurity Frameworks: Firewalls, IDS, SSL
- Authentication: OTPs, biometrics
- Secure Channels: Tokenization, sandbox testing
- Audits & Compliance: GDPR, PCI DSS
- AI Monitoring: Real-time fraud detection
- Customer Education: Alerts, training
- Internal Controls: Role-based access
- Collaboration: Share threat intelligence

For Customers

- Use strong, unique passwords
- Enable 2FA
- Download apps from trusted sources
- Monitor account activity
- Avoid public Wi-Fi
- Install antivirus software
- Report suspicious activity
- Stay informed and cautious

9.6 Emerging Technologies to Combat Fraud

- Blockchain: Immutable transaction records
- Biometric Authentication: Fingerprint, iris, voice
- Real-Time Threat Intelligence: Shared data across banks
- Tokenization: Replace card details with tokens
- Behavioral Biometrics: Detect anomalies via user behavior

9.7 Case Studies

Indian Cases

- Cosmos Bank Cyber Attack (2018): ₹94 crore loss via malware
- PNB Nirav Modi Scam (2018): ₹14,000 crore via fake LoUs
- Yes Bank Fraud (2020): ₹1,000 crore diversion
- Paytm KYC Scam (2020): Social engineering
- VMC Systems Fraud (2021): ₹1,000 crore fraud
- Satyam Scam (2009): Corporate misreporting

International Cases

- Bangladesh Bank Heist (2016): SWIFT system exploited
- Capital One Breach (2019): 100M records exposed
- Wells Fargo Fake Accounts (2016): Internal misconduct
- Equifax Breach (2017): 147M identities stolen
- WannaCry Ransomware (2017): Global disruption

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 9.1

Objective:

Learners will explore and learn how to enable Digital Payment Security Features, including QR code-based payments and Two-Factor Authentication (2FA).

🛠 **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 the selected payment platform

Procedure:

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

Step 2. Assign each group a digital payment app that supports QR code payments.

Step 3. Download and install the assigned app on your smartphone/tablet.

Step 4. Check and set app permissions as discussed in Chapter 6 (e.g., camera access for QR scanning).

Step 5. Explore QR Code Payment Feature:

- Open the app and locate the "Scan & Pay" or "QR Code" option.
- Scan a sample merchant QR code or generate your own QR code for receiving payments.
- Make a small test transaction (₹1 or ₹2) to understand the process.

Step 6. Analyze QR Code Security:

- Discuss how QR codes are encrypted and how apps verify merchant authenticity.
- Identify risks such as fake QR codes and how to avoid them.

Step 7. Document the process:

- Take screenshots of QR scanning, payment confirmation, and QR code generation.
- Note any challenges (e.g., camera permissions, failed scans) and how they were resolved.

Step 8. Present findings:

Each group will prepare slides showing the QR payment process, security features, and suggestions for improvement.

Practical Activity 9.2

Objective:

Learners will explore and learn how to enable Digital Payment Security Features enabling Two-Factor Authentication (2FA).

🛠 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 the selected payment platform

Procedure:

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

Step 2. Assign each group a digital payment platform.

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):

- Log in to your payment account.
- Navigate to “Security Settings” or “Privacy Settings.”
- Enable 2FA using OTP, fingerprint, or face recognition.

Step 6. Set Up Transaction Alerts:

- Go to “Notifications” or “Alerts” section.
- Enable SMS/email/push notifications for every transaction.

Step 7. Enable Encryption and Secure Browsing:

- Check for “https” in the URL if using a browser.
- Enable any app settings related to secure browsing or data encryption.

Step 8. Review and Update Passwords:

- Change your password to a strong one (mix of letters, numbers, symbols).
- Avoid using the same password across multiple platforms.

Step 9. Test the app:

- Log in with and without biometric authentication to compare security.

Step 10. Simulate a phishing attempt (educational purpose only):

- Discuss how phishing works and how 2FA helps prevent unauthorized access.

Step 11. Document and Present:

- Each group will prepare slides with screenshots of security settings.
- Describe each feature enabled and its importance.
- Analyze how the app protects against threats and suggest improvements.
- Note any challenges and how they were resolved.

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.
- **Setting up and Conducting a secure UPI Transaction:** 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
- **To enable Digital Payment Security Features:** 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
- **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. The 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): Real-tie.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

A. Multiple Choice Questions

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

B. 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.

C. 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.

D. 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?

E. 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

A. Multiple Choice Questions

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

B. 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. social engineering, 15. fingerprint

C. True or False

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

Chapter-10

Cyber Crime, Law and Helpline Systems

Gopesh was a 16-year-old student in Bhopal. One evening, while he was doing his homework on his laptop, he got a sudden phone call. The caller introduced himself as an officer from the Cyber Crime Department of Delhi Police. His voice was strict and commanding. Caller: "Your Aadhaar number has been used for illegal activities. We have found your bank account linked to money laundering. If you don't cooperate, you will be arrested immediately." Gopesh froze. He had never done anything wrong! The caller then said that his internet activity would be tracked live, and he must stay on a video call until the "investigation" was over. The scammer warned him not to inform anyone, not even his parents, because "it is a secret case." Then he ordered Gopesh to transfer money to a so-called government account to prove his innocence. Gopesh was frightened and about to send the money when his elder sister walked into the room. She noticed his nervous face on a video call and grew suspicious. Without hesitation, she disconnected the call. She quickly searched online about such scams and found details about the "Digital Arrest" fraud.

They immediately went to the Cyber Crime Police Station and reported the case.The police explained that cybercriminals trick people by pretending to be police officers or government officials. They create fear and digitally arrest victims by keeping them on nonstop video calls until they pay money. Because Gopesh's sister acted on time, no money was lost. The police used his report to alert others about the scam.

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 10.1, 10.2, 10.3, & 10.4. National Crime Records Bureau(NCRB) Report 2023, how cyber crimes are growing year by year in every state of India including

against women & children. 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.

TABLE 9A.5

Police Disposal of Cyber Crime Cases (State/UT-wise) - 2023

SL	State/UT	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]
STATES:						
1	Andhra Pradesh	4381	2341	3	6725	0
2	Arunachal Pradesh	87	24	0	111	0
3	Assam	3270	909	7	4186	0
4	Bihar	3405	4450	0	7855	0
5	Chhattisgarh	417	473	0	890	0
6	Goa	102	86	0	188	0
7	Gujarat	922	1995	0	2917	0
8	Haryana	568	751	0	1319	0
9	Himachal Pradesh	67	127	4	198	0
10	Jharkhand	2674	1079	0	3753	0
11	Karnataka	12446	21889	0	34335	0
12	Kerala	875	3295	6	4176	0
13	Madhya Pradesh	995	685	0	1680	0
14	Maharashtra	16128	8103	0	24231	0
15	Manipur	281	3	0	284	0
16	Meghalaya	173	64	0	237	0
17	Mizoram	11	31	0	42	0
18	Nagaland	11	2	0	13	0
19	Odisha	3200	2348	0	5548	0
20	Punjab	1364	511	0	1875	0
21	Rajasthan	711	2435	0	3146	4
22	Sikkim	28	12	0	40	0
23	Tamil Nadu	3842	4121	30	7993	0
24	Telangana	9179	18236	6	27421	0
25	Tripura	38	36	0	74	0
26	Uttar Pradesh	5645	10794	0	16439	0
27	Uttarakhand	797	494	0	1291	0
28	West Bengal	1155	309	0	1464	0
	TOTAL STATE(S)	**72772**	**85603**	**56**	**158431**	**4**
UNION TERRITORIES:						
29	A&N Islands	27	47	1	75	0
30	Chandigarh	77	23	0	100	0
31	D&N Haveli and Daman & Diu	7	6	0	13	0
32	Delhi	1361	407	0	1768	0
33	Jammu & Kashmir	414	185	70	669	0
34	Ladakh	7	1	0	8	0
35	Lakshadweep	10	1	0	11	0
36	Puducherry	76	147	0	223	0
	TOTAL UT(S)	**1979**	**817**	**71**	**2867**	**0**
	TOTAL ALL INDIA	**74751**	**86420**	**127**	**161298**	**4**

- As per data provided by States/UTs
- States/UTs may not be compared purely on the basis of crime figures

TABLE 9A.5 Page 1 of 4

Figure 10.1 National Crime Records Bureau(NCRB) Report 2023 Volume 2 Page No. 785

TABLE 9A.1

Cyber Crimes (State/UT-wise) - 2021-2023

SL	State/UT	2021	2022	2023	Mid-Year Projected Population (in Lakhs)	Rate of Total Cyber Crimes (2023)	Chargesheeting Rate (2023)
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
STATES:							
1	Andhra Pradesh	1875	2341	2341	532.2	4.4	34.3
2	Arunachal Pradesh	47	14	24	15.7	1.5	2.3
3	Assam	4846	1733	909	358.2	2.5	18.3
4	Bihar	1413	1621	4450	1273.7	3.5	82.7
5	Chhattisgarh	352	439	473	302.9	1.6	84.4
6	Goa	36	90	86	15.8	5.5	30.5
7	Gujarat	1536	1417	1995	717.9	2.8	52.1
8	Haryana	622	681	751	303.3	2.5	62.2
9	Himachal Pradesh	70	77	127	74.8	1.7	71.7
10	Jharkhand	953	967	1079	396.3	2.7	53.4
11	Karnataka	8136	12556	21889	678.3	32.3	18.1
12	Kerala	626	773	3295	358.2	9.2	48.5
13	Madhya Pradesh	589	826	685	869.2	0.8	93.7
14	Maharashtra	5562	8249	8103	1267.1	6.4	31.0
15	Manipur	67	18	3	32.3	0.1	-
16	Meghalaya	107	75	64	33.6	1.9	7.5
17	Mizoram	30	1	31	12.4	2.5	100.0
18	Nagaland	8	4	2	22.4	0.1	16.7
19	Odisha	2037	1983	2348	463.7	5.1	28.3
20	Punjab	551	697	511	308.0	1.7	43.3
21	Rajasthan	1504	1833	2435	813.2	3.0	50.7
22	Sikkim	0	26	12	6.9	1.7	50.0
23	Tamil Nadu	1076	2082	4121	769.4	5.4	60.4
24	Telangana	10303	15297	18236	381.4	47.8	20.9
25	Tripura	24	30	36	41.6	0.9	64.0
26	Uttar Pradesh	8829	10117	10794	2364.8	4.6	45.6
27	Uttarakhand	718	559	494	116.8	4.2	51.2
28	West Bengal	513	401	309	992.4	0.3	80.7
	TOTAL STATE(S)	**52430**	**64907**	**85603**	**13522.4**	**6.3**	**33.7**
UNION TERRITORIES:							
29	A&N Islands	8	28	47	4.0	11.7	85.7
30	Chandigarh	15	27	23	12.4	1.9	31.3
31	D&N Haveli and Daman & Diu	5	5	6	12.9	0.5	83.3
32	Delhi	356	685	407	214.9	1.9	49.0
33	Jammu & Kashmir	154	173	185	136.4	1.4	48.5
34	Ladakh	5	3	1	3.0	0.3	-
35	Lakshadweep	1	1	1	0.7	1.4	-
36	Puducherry	0	64	147	16.6	8.9	100.0
	TOTAL UT(S)	**544**	**986**	**817**	**400.9**	**2.0**	**50.7**
	TOTAL ALL INDIA	**52974**	**65893**	**86420**	**13923.3**	**6.2**	**33.9**

+' 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

Figure 10.2 National Crime Records Bureau(NCRB) Report 2023 Volume 2 Page No. 799

TABLE 9A.10

Cyber Crimes against Women - 2023

SL	State/UT	Cyber Blackmailing / Threatening (Sec.506, 503, 384 IPC r/w IT Act)	Cyber Pornography/ Hosting/ Publishing Obscene Sexual Materials (Sec.67A/67B(Girl Child) of IT act r/w other IPC/SLL)	Cyber Stalking/ Cyber Bullying of Women (Sec.354D IPC r/w IT Act)	Defamation/ Morphing (Sec.469 IPC r/w IPC and Indecent Rep. of Women (P) Act & IT Act)	Fake Profile (IT Act r/w IPC/SLL)	Other Crimes against Women	Total Cyber Crimes against Women
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
STATES:								
1	Andhra Pradesh	10	68	151	1	0	329	559
2	Arunachal Pradesh	0	0	0	0	0	4	4
3	Assam	11	97	2	74	0	285	469
4	Bihar	31	20	75	9	40	469	644
5	Chhattisgarh	3	195	0	0	0	44	242
6	Goa	1	8	0	0	0	19	28
7	Gujarat	9	45	43	0	0	356	453
8	Haryana	6	96	39	1	0	240	382
9	Himachal Pradesh	0	21	2	0	0	17	40
10	Jharkhand	0	12	7	0	0	1	20
11	Karnataka	0	457	4	1	0	6540	7002
12	Kerala	5	333	51	2	29	402	822
13	Madhya Pradesh	12	38	68	2	0	193	313
14	Maharashtra	18	40	415	0	23	2006	2502
15	Manipur	0	0	0	0	0	6	6
16	Meghalaya	0	9	0	1	0	19	29
17	Mizoram	0	0	0	0	0	0	0
18	Nagaland	0	1	0	0	0	0	1
19	Odisha	0	358	0	403	0	0	761
20	Punjab	7	27	14	2	1	76	127
21	Rajasthan	10	212	97	0	3	199	521
22	Sikkim	0	4	0	0	0	4	8
23	Tamil Nadu	14	76	27	1	0	944	1062
24	Telangana	38	78	295	2	2	1032	1447
25	Tripura	0	13	0	0	0	1	14
26	Uttar Pradesh	92	389	18	2	2	960	1463
27	Uttarakhand	26	51	7	0	0	60	144
28	West Bengal	3	6	23	0	0	144	176
	TOTAL STATE(S)	**296**	**2654**	**1338**	**501**	**100**	**14350**	**19239**
UNION TERRITORIES:								
29	A&N Islands	2	27	0	0	0	8	37
30	Chandigarh	0	5	1	0	0	11	17
31	D&N Haveli and Daman & Diu	0	3	0	0	0	0	3
32	Delhi	6	28	18	0	2	81	135
33	Jammu & Kashmir	0	39	1	4	0	24	68
34	Ladakh	0	0	0	0	0	0	0
35	Lakshadweep	0	1	0	0	0	0	1
36	Puducherry	0	10	0	0	0	0	10
	TOTAL UT(S)	**8**	**113**	**20**	**4**	**2**	**124**	**271**
	TOTAL ALL INDIA	**304**	**2767**	**1358**	**505**	**102**	**14474**	**19510**

- As per data provided by States/UTs
- States/UTs may not be compared purely on the basis of crime figures

TABLE 9A.10 Page 1 of 1

Figure 10.3 National Crime Records Bureau(NCRB) Report 2023 Volume 2 Page No. 831

TABLE 9A.1

Cyber Crimes (State/UT-wise) - 2021-2023

SL	State/UT	2021	2022	2023	Mid-Year Projected Population (in Lakhs)	Rate of Total Cyber Crimes (2023)	Chargesheeting Rate (2023)
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
STATES:							
1	Andhra Pradesh	1875	2341	2341	532.2	4.4	34.3
2	Arunachal Pradesh	47	14	24	15.7	1.5	2.3
3	Assam	4846	1733	909	358.2	2.5	18.3
4	Bihar	1413	1621	4450	1273.7	3.5	82.7
5	Chhattisgarh	352	439	473	302.9	1.6	84.4
6	Goa	36	90	86	15.8	5.5	30.5
7	Gujarat	1536	1417	1995	717.9	2.8	52.1
8	Haryana	622	681	751	303.3	2.5	62.2
9	Himachal Pradesh	70	77	127	74.8	1.7	71.7
10	Jharkhand	953	967	1079	396.3	2.7	53.4
11	Karnataka	8136	12556	21889	678.3	32.3	18.1
12	Kerala	626	773	3295	358.2	9.2	48.5
13	Madhya Pradesh	589	826	685	869.2	0.8	93.7
14	Maharashtra	5562	8249	8103	1267.1	6.4	31.0
15	Manipur	67	18	3	32.3	0.1	-
16	Meghalaya	107	75	64	33.6	1.9	7.5
17	Mizoram	30	1	31	12.4	2.5	100.0
18	Nagaland	8	4	2	22.4	0.1	16.7
19	Odisha	2037	1983	2348	463.7	5.1	28.3
20	Punjab	551	697	511	308.0	1.7	43.3
21	Rajasthan	1504	1833	2435	813.2	3.0	50.7
22	Sikkim	0	26	12	6.9	1.7	50.0
23	Tamil Nadu	1076	2082	4121	769.4	5.4	60.4
24	Telangana	10303	15297	18236	381.4	47.8	20.9
25	Tripura	24	30	36	41.6	0.9	64.0
26	Uttar Pradesh	8829	10117	10794	2364.8	4.6	45.6
27	Uttarakhand	718	559	494	116.8	4.2	51.2
28	West Bengal	513	401	309	992.4	0.3	80.7
	TOTAL STATE(S)	**52430**	**64907**	**85603**	**13522.4**	**6.3**	**33.7**
UNION TERRITORIES:							
29	A&N Islands	8	28	47	4.0	11.7	85.7
30	Chandigarh	15	27	23	12.4	1.9	31.3
31	D&N Haveli and Daman & Diu	5	5	6	12.9	0.5	83.3
32	Delhi	356	685	407	214.9	1.9	49.0
33	Jammu & Kashmir	154	173	185	136.4	1.4	48.5
34	Ladakh	5	3	1	3.0	0.3	-
35	Lakshadweep	1	1	1	0.7	1.4	-
36	Puducherry	0	64	147	16.6	8.9	100.0
	TOTAL UT(S)	**544**	**986**	**817**	**400.9**	**2.0**	**50.7**
	TOTAL ALL INDIA	**52974**	**65893**	**86420**	**13923.3**	**6.2**	**33.9**

+' 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

Figure 10.4 National Crime Records Bureau(NCRB) Report 2023 Volume 2 Page No. 832

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.

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 Role of 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 2023 on cyber crime cases disposed of by police in figure 10.2, 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 (Fig. 10.5)

It is a comprehensive platform for reporting various types of cyber crimes.

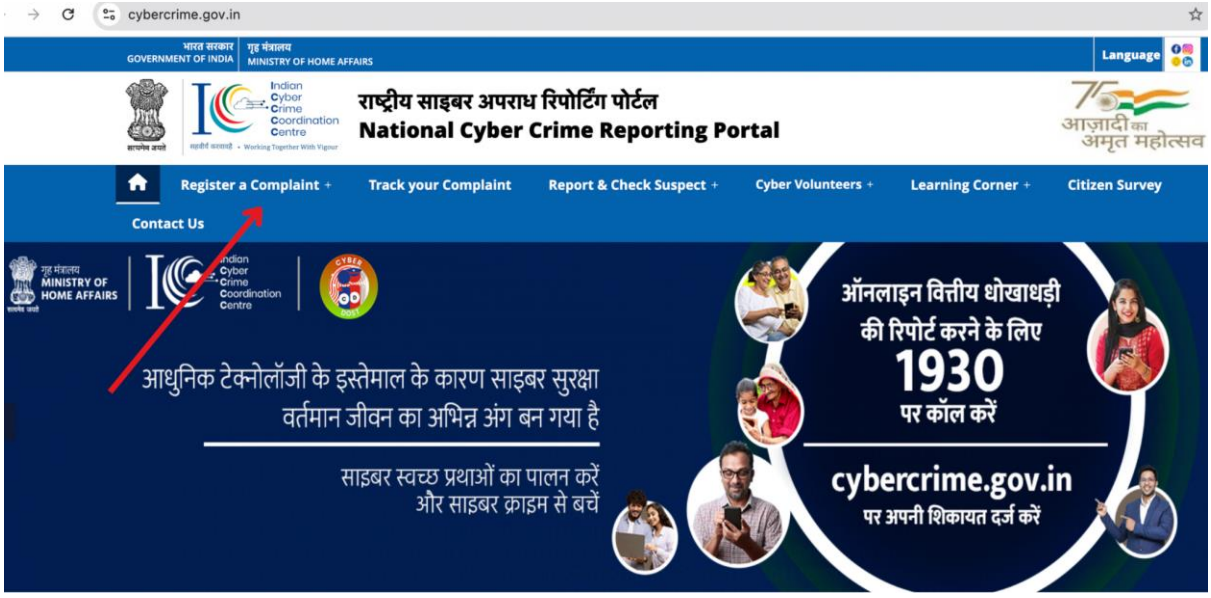


Figure 10.5 Cyber Crime Reporting Portal Home Page

➔ **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 (Figure 10.6). 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

Figure 10.6 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 cyber crime incident by visiting the nearest Cyber Cell office, understanding the procedures, and interacting with officials.

Tools & Platform Needed:

- Notebook and pen for documentation
- Smartphone (optional, for capturing steps or directions)
- Copies of simulated evidence (e.g., screenshots, fake phishing email printouts)

Procedure:

Step 1. Group Formation

- Divide the class into groups of 3–4 students.
- Each group will be assigned a specific type of cyber crime scenario (e.g., phishing, identity theft, fake job offer, cyber defamation, data breach).

Step 2. Scenario Preparation

- Create a simulated cyber crime incident.
- Prepare supporting evidence (screenshots, sample emails, or written descriptions).

Step 3. Scheduling the Visit

- Each group will schedule a visit to the nearest Cyber Cell office.
- Use official police websites or helplines to locate the nearest Cyber Cell.
- Inform the class teacher/facilitator about the planned visit for coordination.

Step 4. Visit the Cyber Cell

- On the scheduled day, groups will visit the Cyber Cell office.
- Meet with the designated officer and explain the simulated incident.
- Provide evidence and ask about the standard procedure for filing a complaint.

Step 5. Reporting Process

- Fill out the required complaint form provided by the Cyber Cell.
- Submit simulated evidence (screenshots, printouts).
- Note down the complaint reference number or acknowledgment slip.

Step 6. Interaction & Follow-Up

- Ask officials about:
    - Common cyber crimes they handle.
    - How complaints are investigated.
    - Response timelines.

- Record answers for classroom discussion.

Step 7. Documentation & Presentation

- Each group documents the entire process:
  - Scheduling the visit
  - Steps taken at the Cyber Cell
  - Interaction with officials
  - Challenges faced and solutions
- Prepare presentation slides with photos (if permitted), notes, and findings.
- Present to the class, highlighting differences between online reporting (Portal) and offline reporting (Cyber Cell visit).

Learning Outcomes

- Learners understand both digital and physical methods of reporting cyber crimes.
- Gain practical exposure to interacting with cyber crime authorities.
- Develop confidence in documenting and presenting real-world processes.

Learn the importance of evidence preservation and proper complaint filing.

Practical Activity 10.2

Objective: Learners will explore and learn how to report a cyber crime 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.

List of other suggested practical activities:

- **Create awareness about cyber crime and cyber safety:** It can be done by making digital posters using Canva/Adobe Express etc.
- **Cyber Safety Checklists:** Prepare Cyber Safety Checklist for school & family members
- **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/files/2CrimeinIndia2023PartII2.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.
- Cyber Crime Investigation Cell: Delhi Police Cyber Crime Unit
- Indian Cyber Crime Coordination Center (I4C): https://i4c.mha.gov.in/

ASSESSMENT

A. Multiple Choice Questions

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) All of the above

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. Which of the following organizations handles cybersecurity incidents in India and provides alerts and advisories?
   a) CERT-In
   b) NCSC
   c) FBI
   d) Interpol

5. 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

6. 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

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. 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

9. 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

10. What is the helpline number for reporting cyber fraud in India?
    a) 112
    b) 1930
    c) 100
    d) 1800

B. 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 National Cyber Crime Reporting Portal is an _____ portal for reporting cyber crimes in India.

C. True or False

1. Skimming devices are used to capture card information at ATMs.
2. The Indian IT Act, 2000, does not address cyber crimes.
3. Denial of Service (DoS) attacks are a type of cyber crime against individuals.
4. Publishing obscene material in electronic form is covered under Section 66 of the Indian IT Act.
5. Cybercrime is a type of traditional crime.
6. The Indian government has established a cyber crime cell to investigate and prosecute cybercrimes.
7. The cyber fraud helpline number in India is 100.
8. The National Cyber Crime Reporting Portal is an offline portal for reporting cyber crimes in India.
9. The IT Act provides penalties for hacking, phishing, and identity theft.
10. Email spoofing is a type of cyber crime against organizations.

D. Short Answer Questions

1. What is cybercrime, and what are its primary categories against individuals, property, organizations, and society?
2. Describe the significance of the Indian IT Act, 2000 in combating cybercrime. Mention at least two advantages of cyber law.
3. Explain the role and importance of Cyber Crime Cells in law enforcement. How does the Cyber Fraud Helpline (1930) assist victims of cyber fraud in India?
4. What is the National Cyber Crime Reporting Portal and how does it help citizens in reporting cybercrime incidents?
5. State the penalties under the IT Act for:
    - Hacking
    - Publishing obscene information in electronic form

E. Long Answer Questions

1. What are the different types of cyber crimes and cyber fraud? Give examples and explain how they affect people, companies, and society.
2. What are the main rules and punishments in the Indian IT Act, 2000? How does this law help protect people from cyber crimes?
3. What are the benefits of cyber law in keeping the internet safe? How do Cyber Crime Cells and helplines help in fighting cyber crimes?

ANSWER KEY

A. Multiple Choice Questions

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

B. Fill in the Blanks

1. Cyber crime, 2. individuals, 3. Hacking, 4. cyber crime, 5. 67, 6. 1930, 7. Cyber crime cells, 8. CERT-In, 9. Cyber terrorism, 10. online

C. True or False

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

PSS Central Institute of Vocational Education

[A constituent unit of NCERT, under the Ministry of Education, Government of India)

Shyamla Hills, Bhopal - 462 002, Madhya Pradesh, India

www.psscive.ac.in