UG S3-01
(SEC)

FOUR YEAR BACHELOR'S DEGREE COURSE

SEMESTER III

CYBER SECURITY

Hiranya Chandra Bhuyan School of Science and Technology

KRISHNA KANTA HANDIQUI STATE OPEN UNIVERSITY

Subject Experts

Prof. Shikar Kumar Sarma, Department of Information Technology, Gauhati University
Prof. Hiren Kumar Deva Sarma, Department of Information Technology, Gauhati University
Dr. Sanjib Kr. Kalita, Department of Computer Science, Gauhati University

Course Co-ordinator : Dr. Ridip Dev Choudhury, KKHSOU
Dr. Tapashi Kashyap Das, KKHSOU
Dr. Sruti Sruba Bharali, KKHSOU

SLM Preparation Team

Units	Authors
1, 2	Dr. Tapashi Kashyap Das, KKHSOU
3, 4, 5	Dr. Sruti Sruba Bharali, KKHSOU
6, 7	Dr. Nabajyoti Sarma, Mahapurush Sankardev University
8,9	Dr. Nabankur Pathak, KKHSOU
10, 11, 14	Dr. Ridip Dev Choudhury, KKHSOU
12, 13	Dr. Santanu Kalita, Mahapurush Sankardev University

Editors

Content : **Dr. Ridip Dev Choudhury,** KKHSOU (Unit 1 to 8)
Dr. Sruti Sruba Bharali, KKHSOU (Unit 9 to 14)

Language : **Dr. Prasenjit Das,** KKHSOU

Structure & Format : **Dr. Nabankur Pathak,** KKHSOU (Unit 1 to 8)
Dr. Tapashi Kashyap Das, KKHSOU (Unit 9 to 14)

Print July, 2024



This Self Learning Material (SLM) of the Krishna Kanta Handiqui State Open University is made available under a Creative Commons Attribution-Non Commercial-Share Alike 4.0 License (international) http://creativecommons.org/licenses/by-nc-sa/4.0/

Printed and published by Registrar on behalf of the Krishna Kanta Handiqui State Open University.

Headquarters: Patgaon, Rani Gate, Guwahati - 781 017
City Campus: NH 37, Resham Nagar, Khanapara, Guwahati - 781 022; www.kkhsou.in

DETAILED SYLLABUS

		Page No
UNIT 1 :	**INTRODUCTION TO CYBERSPACE** Defining Cyberspace and Overview of Computer and Web-technology, Architecture of cyberspace, Communication and web technology.	7-22
UNIT 2 :	**INTRODUCTION TO INTERNET AND CYBER SECURITY** Internet, World wide web, Advent of internet, Internet infrastructure for data transfer and governance, Internet society, Regulation of cyberspace, Concept of cyber security, Issues and challenges of cyber security.	23-43
UNIT 3 :	**CYBER CRIME 1** Classification of cyber-crimes, Common cyber crimes- cyber crime targeting computers and mobiles, cyber crime against women and children.	44-57
UNIT 4 :	**CYBER CRIME 2** Financial frauds, Social engineering attacks, malware and ransomware attacks, zero day and zero click attacks.	58-75
UNIT 5 :	**CYBER LAW** Cybercriminals modus-operandi , Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, Organisations dealing with Cyber crime and Cyber security in India, Case studies.	76-89
UNIT 6 :	**INTRODUCTION TO SOCIAL MEDIA** Introduction to Social networks, Types of Social media, Social media platforms.	90-101
UNIT 7 :	**HANDLING SOCIAL MEDIA** Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social networks.	102-113
UNIT 8 :	**SECURITY ISSUES IN SOCIAL MEDIA** Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices for the use of Social media, Case studies.	114-127

NIT 9 : INTRODUCTION TO E-COMMERCE 128-138
Definition of E- Commerce, Main components of E-Commerce, Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices.

UNIT 10 : INTRODUCTION TO DIGITAL PAYMENTS 139-162
Introduction to digital payments, Components of digital payment and stake holders, Modes of digital payments- Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhaar enabled payments.

UNIT 11 : SECURITY ASPECTS IN DIGITAL PAYMENTS 163-187
Digital payments related common frauds and preventive measures. RBI guidelines on digital payments and customer protection in unauthorised banking transactions. Relevant provisions of Payment Settlement Act,2007.

UNIT 12 : DIGITAL DEVICES SECURITY I 188-211
End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third party software.

UNIT 13 : DIGITAL DEVICES SECURITY II 212-234
Device security policy, Cyber Security best practices, Significance of host firewall and Anti-virus, Management of host firewall and Antivirus.

UNIT 14 : WI-FI SECURITY 235-245
Introduction to Wi-Fi, Types of Wireless security: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA 2), Wi-Fi Protected Access 3 (WPA 3); Threats and risks to Wi-Fi Security, Ways to protect Wi-Fi network, Types of Wi-Fi network security devices, Configuration of basic security policy and permissions.

COURSE INTRODUCTION: CYBER SECURITY

This course on “Cyber Security” comprises of fourteen comprehensive units, designed to provide an in-depth overview of various aspects related to cyberspace and cyber security. As Information Communication Technology (ICT) continues to evolve at an unprecedented pace, the security concerns associated with this growth have become more complex and multifaceted. Consequently, there is an urgent need for a flexible and comprehensive approach to cyber security to effectively address these challenges. The rapid advancement of ICT has led to the proliferation of digital platforms and devices, including social media, e-commerce, digital payments, and other digital services. These developments, while offering numerous benefits, have also introduced a range of security vulnerabilities and threats. Issues such as data breaches, identity theft, cyber fraud, and malicious software attacks are becoming increasingly common, posing significant risks to individuals, businesses, and governments alike. This course aims to address these critical issues by equipping learners with the necessary knowledge and skills to navigate and secure the digital landscape.

One of the primary objectives of this course is to create heightened awareness among digital citizens about the importance of cyber security. By educating users on the various threats and best practices for protecting personal and organizational information, the course aims to foster a culture of vigilance and proactive security measures. The fourteen units of the course cover a broad spectrum of topics, each designed to provide a holistic understanding of cyber security. These units delve into the foundational principles of cyber security, the types of cyber threats and attacks, and the methods used to prevent and respond to such incidents. Topics such as cybercrimes, cyber law, security issues in social media and digital payments, and issues related to security aspects in digital devices and Wi-Fi-security are explored in detail, offering learners a well-rounded education in the field.

Each unit of these blocks includes some along-side boxes to help you know some of the difficult, unseen terms. Some “ACTIVIITY” have been included to help you apply your mind. You may find some boxes marked with: “LET US KNOW”. These boxes will provide you with some additional interesting and relevant information. Again, you will get “CHECK YOUR PROGRESS” questions. These have been designed to self-check your progress of study. It will be helpful for you if you solve the problems put in these boxes immediately after you go through the sections of the units and then match your answers with “ANSWERS TO CHECK YOUR PROGRESS” given at the end of each unit.

UNIT 1: INTRODUCTION TO CYBERSPACE

UNIT STRUCTURE

1.1 Learning Objectives

1.2 Introduction

1.3 Introduction to Cyberspace

1.4 Architecture of Cyberspace

1.5 Overview of Computer

1.5.1 Characteristics of Computers

1.5.2 Basic Components of a Computer

1.6 Overview of Web Technology

1.6.1 World Wide Web

1.7 Let Us Sum Up

1.8 Answers to Check Your Progress

1.9 Further Reading

1.10 Model Questions

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- learn the concept of cyberspace,understanding its scope, significance, and impact on modern society.
- learn about the architecture of cyberspace that support the seamless functioning of digital communications and online activities.
- familiarize yourself with the essential aspects of computers, including their characteristics, fundamental components, and functionalities.
- acquire an overview of web technology and its various related technologies.

1.2 INTRODUCTION

This is the first unit of the Cyber Security course we will start with the basics, beginning with the definition of cyberspace. We will explore its structure, the role of communication and web technologies, and its impact on communication, commerce, education, and society.

Next, we will cover the basics of computer systems, including their features, functions, and main components. Then, we will move on to web technology, focusing on the World Wide Web. We will explain how the web is organized and how it supports online interactions and activities.

1.3 INTRODUCTION TO CYBERSPCACE

The term “cyberspace” was first coined by science fiction writer *William Gibson* in his 1984 novel “*Neuromancer*”. Although Gibson’s depiction was fictional, it portrayed cyberspace as a virtual world created by connected computer networks. Cyberspace has many interpretations but generally refers to the virtual environment formed by interconnected computers, servers, and networks. It is a place where digital communication, data exchange, and online activities occur.

Cyberspace encompasses more than just the Internet. It includes all forms of digital communication and the virtual environments where data is stored and processed. This space is not constrained by physical locations, enabling instant global communication and data exchange. Despite lacking a physical presence, cyberspace profoundly impacts the modern world, transcending national boundaries. It serves as a platform where information is transmitted, received, stored, and processed. Many people spend significant time in cyberspace, sharing information, interacting, playing games, and engaging in social forums. Various industries, such as education, finance, marketing, and entertainment, heavily rely on cyberspace. Organizations also use it extensively to store and manage their data.

Activities like accessing data on phones and computers, internet banking, online shopping, booking appointments, and purchasing tickets

have become easier. For example, during the COVID-19 crisis, online education allowed teachers and students to connect remotely, maintaining social distancing while continuing classes. This was possible for those with internet access and a device. Online gaming is another example, where people from different locations connect and play together digitally. Nowadays, many employees work from home, using the internet for communication and data access. Students and children also use the internet for learning and entertainment.

1.4 THE ARCHITECTURE OF CYBERSPACE

The architecture of cyberspace consists of several layers, each serving a critical function in enabling communication and data exchange.It consists of various components that work together to enable digital communication and data exchange. The architecture includes the physical infrastructure, software systems, protocols, and regulatory frameworks that enable and govern interactions in cyberspace. These components can be broadly categorized into fourconceptual layers:*physical layer, network layer, application layer,* and *social layer.*

- At the foundational level, we have the ***physical layer***, which includes the hardware. It includes all the tangible components that form the infrastructure of digital communication. This layer encompasses:

  Hardware: It includes the computers, servers, routers, switches, and cables that form the backbone of the internet, enabling data transmission across the globe.

  Data Centres: Data centres provide the facilities of servers, storage systems, and networking equipment essential for hosting websites, applications, and data.
- The ***network layer*** is built on top of the physical layer and includes the protocols and technologies that enable data to be transmitted across the infrastructure. Key components of network layer are:

  Internet Protocol (IP): It is the primary protocol for routing data packets across the Internet.

Transmission Control Protocol (TCP): The TCP ensures reliable data transmission between devices.

- The ***application layer*** is where user interactions with cyberspace occur. It includes: w*eb browsers, email clients, social media platforms, online services.*

  Web Browsers are software applications that allow users to access and interact with websites.

  Email Clients are programs used to send and receive emails.

  Social Media Platforms are Websites and applications that enable users to create and share content and participate in social networking.

  Online Services include E-commerce platforms, cloud services, streaming services, and other applications that provide various functionalities over the Internet.

- The ***social layer*** encompasses the human element of cyberspace, including the users and the societal structures that emerge from digital interactions. This layer includes:

  User Communities i.e., the groups of individuals who interact and communicate within cyberspace.

  Cultural Norms: The behaviours, practices, and values that develop within digital communities.

  Legal and Regulatory Frameworks: Laws and regulations that govern online activities and protect users' rights and privacy comes under this.

To grasp the intricate frameworks of cyberspace, it is helpful to get a clear picture of how computers and web technologies function to ensure seamless and efficient online operations. The following sections will provide an overview of computer and web technology.

1.5 OVERVIEW OF COMPUTER

Computers have become an integral part of modern society, influencing almost every aspect of our lives. From personal use at home to essential roles in education, businesses, healthcare, and beyond, computers help us

to work more efficiently, communicate effectively, and solve complex problems. This section will provide an overview of what computers are, their characteristics,main components, and functionalities of computer.

Definition of Computer:

A computer is an *electronic device* that processes data and performs tasks according to a set of instructions, known as programs or software. It is designed to carry out complex calculations, manage data, and perform a wide range of tasks quickly and accurately.

In the past, computers were extremely large and often required an entire room for installation. These machines consumed enormous amounts of power and were too expensive for commercial use. Consequently, they were limited to specialized tasks, such as calculating trajectories for astronomical or military purposes. However, with technological advancements, computers became smaller and their energy requirements decreased significantly. This development paved the way for their adoption in commercial applications. Today, computers are so widespread that they are integral to various interactive devices such as cell phones, global positioning system (GPS) units, automatic teller machines (ATMs), and more.

1.5.1 Characteristics of Computers

A computer is an electronic device that operates based on a set of instructions called a program. It accepts data, processes it, and generates information. In this context, data refers to raw facts or figures, while information denotes the processed data.

Computer are basically meant to solve problems quickly and accurately. The main characteristics of a computer are: ***Speed, Storage, Accuracy, Automation, Diligence, Versatility,*** and ***Cost effectiveness***. Understanding these characteristics is crucial in the field of cyber security.

- **Speed:** One of the most notable characteristics of a computer is its speed. Computers can process data and execute instructions at incredible speeds. The speed of computer sis

usually given in nanoseconds and picoseconds, where 1 nanosecond = 1×10^{-9} seconds and 1 picosecond =1×10^{-12} seconds. This speed allows computers to perform complex calculations and tasks quickly, making them indispensable in fields like scientific research, financial modeling, and real-time systems.

- **Storage:** Computers, like humans, have memory. Just as we can't retain everything in our minds and rely on secondary media like notebooks to record important information, computers use both internal (primary) and external (secondary) memory. Internal memory is costly and limited in capacity, whereas secondary storage is more affordable and offers greater capacity. Secondary memory is crucial for data storage. Examples of secondary storage include hard disk drives (HDDs), solid-state drives (SSDs), optical disks (CDs and DVDs), and pen drives.
- **Accuracy:**A computer is a fast, reliable, and robust electronic device that always produces accurate results, given that the correct data and instructions are provided. Therefore, if an error occurs, it is the responsibility of the user who entered the incorrect data or program. This demonstrates that the output of a computer depends on the instructions and input data it receives. In computer terminology, this principle is known as "garbage-in, garbage-out."
- **Automation:** Automation in computers refers to a system's ability to perform a sequence of operations or tasks without human intervention once the instructions or program are set. This capability allows computers to execute predefined commands systematically and accurately, increasing efficiency, reducing human error, and freeing up human resources for more complex tasks. Automation enhances productivity, accuracy, and efficiency across various domains, including cybersecurity.
- **Diligence:**Unlike humans, computers never get tired of repetitive

tasks. They can work continuously for hours without making errors. Regardless of the number of executions required, each one takes the same amount of time and is performed with consistent accuracy.

- **Versatility:** Computers are capable of performing a wide range of tasks. Versatility, the quality of being *flexible*, allows computers to be used in various fields of daily life. For example, they serve as personal computers for home use, educational tools, business aids, teaching aids,weather forecasting systems, complex simulations, and tools in railways, banking, medicine, and entertainment. This demonstrates their ability to handle different tasks simultaneously. The multi-processing capabilities of computers make them inherently versatile, allowing easy adaptation to any field.
- **Cost effectiveness**: Using computers reduces the need for manpower and provides an elegant and efficient way to perform various tasks. For example, sending an important document via the conventional postal system takes at least 2-3 days, while the same information sent through email is delivered instantly. This reduces paperwork and human effort, thereby lowering costs.

Although the trend today is to make computers intelligent by incorporating Artificial Intelligence (AI), they still lack independent decision-making abilities. Their intelligence level is essentially zero, and they need guidance to perform tasks.

1.5.2 Basic Components of a Computer

For a computer to operate smoothly, hardware and software must work together seamlessly. The operating system acts as an intermediary, enabling software to interact effectively with hardware resources. Before we talk about the basic parts of a computer, it's important to understand its hardware and software.

Computer hardware refers to the physical components that

make up a computer system, which are tangible and can be seen and touched. It includes essential parts like the CPU, RAM, input/output devices, and storage components, each playing a specific role in the computer's overall operation.

On the other hand, **computer software** refers to a collection of instructions, data, or programs that enable computers to perform tasks. Unlike hardware, software is intangible. It can be broadly categorized into two types:

- **System software**
- **Application software**

System software manages and supports computer hardware, providing a platform for other software to run effectively. This category includes *operating systems* (such as Windows, Linux, and macOS), *device drivers* (which facilitate communication between hardware and the OS), and *utilities* (programs for tasks like virus scanning and disk maintenance).

Application software, meanwhile, is designed to help users carry out specific tasks. Examples include productivity software (like word processors and spreadsheets), media players and editors (for audio, video, and images), web browsers (such as Google Chrome, Firefox, etc), and games for entertainment purposes.

Understanding the various components of a computer is crucial to grasping how it operates. Let us discuss the primary components very briefly.

1. **Central Processing Unit (CPU):** The CPU, often called the brain of the computer, is responsible for executing instructions and performing calculations. It processes data and manages the flow of information throughout the computer. A faster CPU enables quicker execution of program instructions, leading to improved overall performance.
2. **Memory:Random Access Memory (**RAM) is a type of volatile memory used by the computer to store data that is actively being used or processed by the CPU. This temporary data is lost when

the computer is turned off. RAM allows for quick read and write access, enhancing overall performance. A fast CPU is ineffective without sufficient RAM, as it provides the necessary space for running multiple applications simultaneously without degrading system performance.

3. **Read Only Memory (ROM):** Permanent storage that contains essential instructions for booting the computer and performing basic operations.
4. **Storage:** Storage devices, such as Hard Disk Drives (HDDs) and Solid-State Drives (SSDs), are used to store data permanently. These devices hold all types of data, including documents and programs. The larger the storage capacity, the more data can be saved on the device.
5. **Motherboard:**The motherboard is the main circuit board that connects all components of the computer, allowing them to communicate with each other. The motherboard is a printed circuit that has connectors for expansion cards, memory modules, the processors, etc.
6. **Input Devices:** Input devices allow users to interact with and control a computer. These devices enable the user to input data, commands, and responses, facilitating communication with the system. Common examples include keyboards,mouse,and touchscreens. Other input devices include scanners, which digitize physical documents, and microphones, which capture audio input for voice commands and recording.
7. **Output Devices:** Output devices are hardware components that convey the results of a computer's processing to the user. They translate digital information into a form that can be perceived, whether visually, audibly, or physically. Common output devices include:

- **Monitors**: Display visual output from the computer, including text, images, and videos.

- **Printers**: Produce physical copies of digital documents and images.
- **Speakers**: Convert digital audio signals into sound.
- **Projectors**: Display visual content on large screens for presentations and multimedia displays.
- **Headphones**: Provide personal audio output with improved sound quality.

8. **Power Supply Unit (PSU):** The PSU converts electrical power from an outlet into a usable form for the computer and its components.

Functionalities of a Computer:

The main functionalities of a computer are as follows:

- **Data Processing:** Computers process data by performing calculations, sorting information, and manipulating data according to the instructions in software programs.
- **Data Storage:** Computers store data both temporarily in RAM and permanently on storage devices. This includes everything from system files to user documents.
- **Networking:** Computers can connect to other computers and devices through wired or wireless networks, enabling data sharing, internet access, and communication.
- **User Interface:** Computers provide interfaces for users to interact with them, such as Graphical User Interfaces (GUIs) and Command-Line Interfaces (CLIs).
- **Automation:** Computers can automate repetitive tasks through programming, increasing efficiency and reducing the potential for human error.

1.6 OVERVIEW OF WEB TECHNOLOGY

Web technology encompasses the tools and techniques used for communication between different devices via the Internet. It facilitates the creation, management, and delivery of web content using languages like HTML, JavaScript, PHP, and others. The Internet hosts numerous public

websites, each consisting of web pages containing information in text, video, audio, and image formats. These resources are interconnected through hyperlinks on the World Wide Web, accessible through software interfaces provided by web browsers.

Understanding web technology is crucial for studying cyberspace because it describes how information is shared and accessed online. **Web browsers**, such as Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, and Internet Explorer, play a vital role in displaying text, data, pictures, animations, and videos from the Internet. They provide the interface through which users interact with and navigate through web content, making them essential tools for exploring and comprehending the digital landscape of cyberspace.

A **web server** refers to a computer or a network of computers designed to deliver web pages and content to multiple users. It processes requests from users over the network and provides them with files that create web pages. Essentially, a web server is a software application that fulfils requests for web pages, aiming to store, process, and deliver content efficiently. This interaction occurs through the Hypertext Transfer Protocol (HTTP).

On the web, all the documents are formatted in a special markup language called *hypertext markup language* (HTML), which supports links to other documents, graphics, audio, and video files. Web servers primarily handle content such as HTML documents, images, style sheets, and text. Besides HTTP, they also support protocols like SMTP (Simple Mail Transfer Protocol) for email and FTP (File Transfer Protocol) for file storage and transfer. When a client requests a web page, the server responds by either sending the requested file directly or by dynamically generating a response through scripts that interact with databases.Popular examples of web servers include *Apache Web Server, Microsoft's Internet Information Services* (IIS), Apache Tomcat, and *NGINX*.

1.6.1 World Wide Web

The terms Internet and Web are now commonplace. The **World Wide Web** (WWW), often referred to simply as the Web, is a crucial

service provided by the Internet. It serves as a global platform for organizing and presenting a wide range of written, graphical, and audio-visual information from around the world. Alongside the Web, popular Internet services include email, Telnet, FTP, and e-commerce.The Web enables various activities:

- Searching for information on topics such as news, e-papers, schedules, eBooks, current events, science, technology, and politics.
- Sharing information globally.
- Conducting online banking transactions and investments.
- Downloading software and applications.
- Sending emails and official correspondence.
- Uploading and downloading files, software, music, and videos.
- Accessing remote computers, information services, participating in online discussions, video conferencing, and chatting.

The World Wide Web was invented by British scientist **Tim Berners-Lee** at CERN (European Organization for Nuclear Research) in Switzerland in 1989. He also developed three foundational technologies in 1990: Hypertext Transfer Protocol (HTTP) for retrieving hyperlinked resources, Uniform Resource Identifier (URL) for identifying resources on the Web, and Hypertext Markup Language (HTML) for designing webpages using tags that define structure, organization, and content.

LET US KNOW



Let us talk about something beyond the regular web which need to be worried about. The websites we visit every day for the sake of information represent just a small fraction of the whole the Internet. The Internet is structured into layers: the surface web, the deep web, and the dark web.

Surface Web: This is the most visible and accessible part of the internet that we use daily. It consists of websites indexed by search engines like Google and Bing. These websites contain information ranging from news and entertainment to educational resources and e-commerce platforms.

Deep Web: The deep web constitutes a larger portion of the internet than the surface web. It includes content that is not indexed by search engines and requires specific URLs or credentials to access. Here, youwilll find data such as private databases, medical records, financial information, and academic resources that are not intended for public access.

Dark Web: The dark web is intentionally hidden and requires special tools or software, like TOR (The Onion Router) or I2P (Invisible Internet Project), to access. It operates on an overlay network that anonymizes users by masking their IP addresses through multiple layers of encryption. The dark web is known for hosting illicit activities and content, including illegal trade, hacking services, illicit pornography, drug trafficking, and extremist ideologies. It is designed to provide anonymity and privacy to users, making it challenging for authorities to trace activities conducted within this realm of the internet.

In this unit, we introduced the complex world of cyberspace. We have described its broad scope, importance, and deep impact on modern society.



CHECK YOUR PROGRESS

Q1) What does the physical layer of cyberspace include?

Q2) What is the primary function of the network layer in cyberspace?

Q3) Name two key components of the network layer.

Q4) What is the role of web browsers in the application layer?

Q5) What types of platforms are included in the social layer of cyberspace?

Q6) What are data centres, and what do they provide?

Q7) Define Internet Protocol (IP) in the context of the network layer.

Q8) Describe how the versatility of computers allows them to be used in various fields of daily life.

Q9) Explain the main characteristics of computers that make them indispensable in various fields.

Q10) Fill in the blanks:

i. The _____ includes websites filled with data which isindexed by search engines.

ii. The _____refers to the Internet that is intentionally hidden.

iii. The term “cyberspace” was first coined by science fiction writer _____ in his novel _____.

iv. _____ includes content that is not indexed by search engines and requires specific URLs or credentials to access.



1.7 LET US SUM UP

- Cyberspace is a virtual environment formed by interconnected computers, servers, and networks, enabling digital communication and activities.
- It expands with the use of smartphones and IoT devices, supporting virtual meetings, online counselling, and business deals.
- Cyberspace encompasses computers, networks, data storage, websites, emails, and ATMs, and is vital for education, finance, marketing, and entertainment.
- Its architecture includes several layers: physical (hardware), network (protocols like IP and TCP), application (web browsers, email clients, online services), and social (user communities, cultural norms, legal frameworks).
- Computers process data and perform tasks efficiently, characterized by speed, storage, accuracy, and versatility.
- Web technology enables communication over the Internet, with the World Wide Web (WWW), created by Tim Berners-Lee in 1989, facilitating activities such as information searching, online banking, software downloading, emailing, file sharing, remote access, and online discussions.



1.8 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q1: The physical layer includes hardware such as computers, servers, routers, switches, and cables, as well as data centres that host servers, storage systems, and networking equipment.

Answer to Q2: The network layer includes protocols and technologies that enable data to be transmitted across the infrastructure.

Answer to Q3: Internet Protocol (IP) and Transmission Control Protocol (TCP).

Answer to Q4: Web browsers are software applications that allow users to access and interact with websites.

Answer to Q5: The social layer includes user communities, cultural norms, and legal and regulatory frameworks.

Answer to Q6: Data centres provide facilities for servers, storage systems, and networking equipment essential for hosting websites, applications, and data.

Answer to Q7: Internet Protocol (IP) is the primary protocol for routing data packets across the Internet.

Answer to Q8:Versatility, the quality of being flexible, allows computers to be used in many fields such as home use, education, business, weather forecasting, simulations, banking, medicine, and entertainment. Their multi-processing capabilities enable them to handle different tasks simultaneously, adapting easily to any field and increasing their applicability in diverse areas.

Answer to Q9: The main characteristics include speed, storage, accuracy, automation, diligence, versatility, and cost-effectiveness. These characteristics allow computers to process data quickly, store large amounts of data, perform tasks accurately, automate repetitive tasks, work tirelessly without errors, adapt to various tasks, and reduce operational costs.

Answer to Q10: i) surface web ii) dark web

iii) William Gibson, Neuromancer iv) Deep web



1.9 FURTHER READING

1) Sunit, B., & Nina, G. (2011). Cyber Security: Understanding Cybercrimes, computer forensics and Legal Perspectives. *Wiley India*.
2) Cole, E. (2011). *Network security bible*. John Wiley & Sons.
3) Maiwald, E. (2003). *Fundamentals of network security*. Dreamtech press.
4) https://wisdomplexus.com/blogs/secure-cyberspace/
5) https://www.kaspersky.com/resource-center/threats/deep-web
6) https://keerthicomputerstudymaterials.files.wordpress.com/2016/10/chapter-1-overview-of-computer.pdf



1.10 MODEL QUESTIONS

Q1. What does cyberspace generally refer to?
Q2. How does cyberspace enable global communication?
Q3. What are the basic components of a computer system and how do they interact?
Q4. What are the characteristics of computer?
Q5. Mention the functional components of a computer.
Q6. What is web browser and a web server? Give examples.
Q7. Write short notes on World Wide Web.
Q8. What are some common activities enabled by the WWW?
Q9. Who coined the term “cyberspace,” and in which novel did he introduce it?
Q10. How do web browsers interpret and display web content?
Q11. Describe the architectural layers of cyberspace.
Q12. What components make up the physical layer of cyberspace architecture?
Q13. What does the social layer of cyberspace encompass?
Q14. What is surface, deep and dark web?
Q15. Discuss the role and importance of the physical layer in the architecture of cyberspace. Include examples of key components.

*** ***** ***

UNIT 2: INTRODUCTION TO INTERNET AND CYBER SECURITY

UNIT STRUCTURE

2.1 Learning Objectives

2.2 Introduction

2.3 Internet

- 2.3.1 Advent of Internet
- 2.3.2 Internet Infrastructure for Data Transfer and Governance
- 2.3.3 Internet Society

2.4 Importance and Impact of Internet in Society

2.5 Challenges and Concern

2.6 Regulations in Cyberspace

2.7 Concept of Cyber Security

- 2.7.1 Issues and Challenges of Cyber Security

2.8 Let Us Sum Up

2.9 Answers to Check Your Progress

2.10 Further Reading

2.11 Model Questions

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- gain an overview of the Internet
- learn about Internet infrastructure
- learn about the Internet Society, its mission, and activities
- explore the fundamental concepts of cybersecurity
- discuss regulations in cyberspace
- identify and discuss the challenges faced by cybersecurity

2.2 INTRODUCTION

In the previous unit, we provided an overview of computer and web technology. We explored cyberspace, a virtual environment where people

spend much of their time today, along with the World Wide Web and various related technologies.

In the realm of information technology, data security is crucial. This unit offers an overview of Internet and Cyber Security. We begin with the origins of the Internet and its infrastructure for data transfer and governance. Then, we define cyber security and discuss the need for regulations in cyberspace. This unit will also describe the concept of cyber security, examining its issues and challenges.

2.3 INTERNET

After the invention of the computer in the 20th century, the advent of the Internet can be considered a giant leap for Information Technology. In simple terms, the Internet is a network of networks that connects people and computers worldwide. The term “Internet,” often referred to as “the Net,” is now very common and has become a vital part of our lives, enabling global connectivity. With the Internet, we can share information across the world, make friends, listen to music, watch movies, pay bills, order items, and greet friends and relatives, among many other activities.

Now let us discuss what the Internet is.The Internet is a vast global network of interconnected computers and other devices that communicate and share information using standardized protocols. The Internet connects millions of private, public, academic, business, and government networks worldwide. This interconnected web of networks allows devices from all over the globe to communicate with each other. The Internet has a broad scope and thus is defined differently by various groups of people.

The operation of the Internet relies on a combination of components and virtual resources divided into three layers: **physical**, **transport**, and **application**. The physical layer encompasses the wired and wireless telecommunications infrastructure used for transferring data among various connected devices. The transport layer includes essential Internet protocols and standards, such as TCP/IP, DNS, and the World Wide Web, which facilitate data exchange across networks. The Internet operates using a

suite of protocols known as TCP/IP (Transmission Control Protocol/Internet Protocol). These protocols define how data is transmitted and received over the network, ensuring reliable and standardized communication between devices.The application layer consists of the applications running on the Internet that provide diverse services to users.

2.3.1 Advent of Internet

The origins of the Internet can be traced back to the early 1960s, a period marked by significant technological advancements. During this time, the U.S. Department of Defense's *Advanced Research Projects Agency* (ARPA) sought to develop a robust, fault-tolerant communication system that could withstand potential military attacks. This initiative led to the creation of **ARPANET** (Advanced Research Projects Agency Network), a pioneering project that laid the groundwork for the modern internet. The primary goal of ARPANET was to facilitate reliable communication between computers located at different universities and research institutions, fostering collaboration and information sharing among scientists and researchers.

Transition to TCP/IP

The development of key protocols, such as the Network Control Protocol (NCP) and later the Transmission Control Protocol/Internet Protocol (TCP/IP), further enhanced ARPANET's capabilities, enabling more efficient and reliable data transmission. In the 1970s, the Transmission Control Protocol (TCP) and Internet Protocol (IP) was developed, which became the backbone of Internet communication. TCP/IP allowed diverse networks to interconnect and communicate, forming the basis of the modern internet.

By the early 1980s, ARPANET had transformed into a sophisticated network that connected not only academic and research institutions but also served as a testing ground for innovative networking technologies. This evolution laid the groundwork for the expansive, interconnected Internet we know today, demonstrating the potential

for widespread digital communication and collaboration.By 1983, ARPANET had fully transitioned to TCP/IP, setting the stagefor global connectivity.

The World Wide Web (WWW), invented by **Tim Berners Lee** in 1989, revolutionized the Internet.In the late 1980s, the National Science Foundation (NFS) of U.S. funded the development of a network named NSFNET to connect super computer centres in the United States. Many universities and institutions were encouraged to connect to the network. Creation of NSFNET was the first large-scale implementation of Internet technologies in a complex environment of many independently operated networks.These large worldwide connections of networks and computer systems communicating according to the same protocols is what we called Internet. Commercial firms noted the popularity and effectiveness of the growing Internet and built their own networks. In the early 1990s, commercial networks with their own Internet exchanges or gateways were allowed to conduct business on the Internet. The direct role NFS in the Internet ended in the year 1998. In that year, the network functions were transferred to the commercial sector.

2.3.2 Internet Infrastructure for Data Transfer and Governance

The internet infrastructure for data transfer and governance is a complex and dynamic field that requires constant evolution to meet the demands of users and comply with regulatory standards. It involves various layers and components, including physical hardware, software, protocols, data centres, services, and governance frameworks.

1. Physical Infrastructure

Physical infrastructure includes all the hardware components. Networking hardware encompasses components such as routers, switches, fiber optic cables, undersea cables, and wireless access points. Undersea cables are large-scale fiber optic cables laid on the

ocean floor, connecting continents and enabling global data transfer. These elements are crucial for the physical transmission of data across local, regional, and global networks. By facilitating seamless data flow, networking hardware ensures robust and efficient connectivity, enabling the vast exchange of information that powers the Internet.

2. Data Transfer Protocols

Data transfer protocols are essential for the smooth operation of the Internet, enabling reliable and secure communication. **Transmission Control Protocol/Internet Protocol** (**TCP/IP**) is foundational, with **TCP** ensuring reliable data transmission through connection establishment and error-checking, while **IP** handles the addressing and routing of packets to ensure data reaches its intended destination. **Hypertext Transfer Protocol** (**HTTP**) is the core protocol for data communication on the World Wide Web, with **HTTPS** being its secure version that adds encryption mechanism. **File Transfer Protocol** (FTP) facilitates the transfer of files between a client and server over a network, making it easier to move large amounts of data. Other important protocols include **Simple Mail Transfer Protocol** (SMTP), which is used for email transmission, and **Domain Name System** (DNS), which translates domain names into IP addresses, enabling easier navigation of the web. These protocols collectively ensure efficient, reliable, and secure data transfer across the internet.

3. Data Centers and Cloud Infrastructure

Data centres are critical facilities covering servers, storage devices, and networking equipment, forming the backbone of Internet infrastructure. They provide the essential physical space and power required for data processing and storage. Cloud providers like Amazon Web Services (AWS), Google Cloud, and Microsoft Azure offer scalable computing resources and storage over the Internet.

4.Data Governance

Data governance encompasses regulatory frameworks, data management policies, and standards and best practices.Data

governance, particularly within regulatory frameworks, focuses on establishing rules and standards to govern how organizations manage and protect data. One of the prominent regulations in this field is the *General Data Protection Regulation* (GDPR), implemented by the European Union (EU). GDPR is a comprehensive law that aims to safeguard the personal data of individuals within the EU and regulate its processing. It sets stringent guidelines for data collection, storage, and usage, emphasizing transparency, accountability, and the rights of individuals over their personal information.In addition to GDPR, another significant regulatory framework is the *California Consumer Privacy Act* (CCPA), which was enacted at the state level in the United States. CCPA enhances privacy rights and consumer protections for residents of California, offering them greater control over their personal information held by businesses.

Data management policies focus on data privacy, ensuring that personal data is collected, stored, and processed in compliance with privacy laws. These policies also emphasize data security by implementing measures to protect data from unauthorized access, breaches, and other cyber threats, and they ensure data integrity by maintaining the accuracy and consistency of data throughout its lifecycle.

Standards and best practices are vital for effective data governance.The *National Institute of Standards and* Technology (NIST) Cybersecurity Framework offers guidelines for managing cybersecurity risks, helping organizations strengthen their data protection measures. Together, these elements create a comprehensive approach to managing and safeguarding data in today's digital landscape.

By leveraging advanced technologies and adhering to best practices, organizations can ensure efficient, secure, and compliant data management and transfer.

2.3.3 Internet Society

Due to the emergence of the World Wide Web in late 1990 the Internet is growing day-by-day worldwide. Not only the spread of Internet, but mobile and wireless networks are too equally important to the spread of the Internet. Recent developments in the multimedia applications such as voice over IP, video over IP, television over IP has increased the number of users extensively and the amount of time each user spends on the network. For monitoring such a huge network, there is a necessity of an international body which can frame the rules and regulations, protocols to join and use the network. In 1992, an international organization, known as the "The Internet Society" was formed to take care of such issues.

The Internet Society is a global non-profit organization empowering people to keep the Internet secure while exchanging information. The goal of the organization is to keep the Internet to be open, globally connected, secure, and trustworthy so that peoples from all the corners of the world could collaborate.The mission and the various activities of the organization is available in the official website https://www.internetsociety.org/.

As per the official website of the organization, the mission of the Internet Society and the activities of the society are as follows:

Vision	The Internet Is for Everyone
Mission	The Internet Society supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society.
Highlights of Activities	The Internet Society: • Facilitates open development of standards, protocols, administration, and the technical infrastructure of the Internet. • Supports education in developing countries specifically, and wherever the need exists.

	• Promotes professional development and builds community to foster participation and leadership in areas important to the evolution of the Internet. • Provides reliable information about the Internet. • Provides forums for discussion of issues that affect Internet evolution, development and use in technical, commercial, societal, and other contexts. • Fosters an environment for international cooperation, community, and a culture that enables self-governance to work. • Serves as a focal point for cooperative efforts to promote the Internet as a positive tool to benefit all people throughout the world. • Provides management and coordination for on-strategy initiatives and outreach efforts in humanitarian, educational, societal, and other contexts.

Source: https://www.internetsociety.org/

2.4 IMPORTANCE AND IMPACT OF INTERNET IN SOCIETY

The Internet has profoundly impacted society across several dimensions:

- **Communication and Connectivity:** It has revolutionized communication, enabling instant and global interaction through platforms such as email, social media, and instant messaging. Video conferencing tools have bridged geographical gaps, facilitating real-time face-to-face interactions.
- **Access to Information:** The internet has democratized access to knowledge with search engines, online libraries, and databases. It empowers individuals to learn about diverse topics from anywhere with an internet connection, fundamentally reshaping how information is accessed and shared.
- **E-Commerce**: Significantly boosting economic growth, the internet

has spawned new industries and job opportunities. Online shopping platforms like Amazon and eBay have transformed retail by offering global access to goods. Digital payments and online banking have made financial transactions more efficient and convenient.

- **Education and E-Learning**: In education, the internet has brought about a revolution with online courses, virtual classrooms, and educational resources accessible globally. Platforms such as Coursera, Khan Academy, and edX provide courses from prestigious institutions to learners worldwide.
- **Entertainment:** Online gaming, social media, and digital content creation have introduced new forms of entertainment and avenues for self-expression. Streaming services like Netflix, YouTube, and Spotify have revolutionized how people consume media, offering vast libraries of content at their fingertips.
- **Social Impact:** The Internet has empowered social movements and activism by amplifying voices and facilitating the organization of protests and campaigns through social media platforms. It has become a powerful tool for social change and community engagement on a global scale.

The Internet continues to evolve, with emerging technologies like theInternet of Things (IoT), 5G technology, and Artificial Intelligence(AI) set to further transform our lives.

2.5 CHALLENGES AND CONCERNS

The Internet, despite its many benefits, also introduces several challenges. Some of them are:

Privacy: One major concern is privacy. The collection and potential misuse of personal data by companies and governments raise significant ethical and legal issues.

Security: Cybersecurity remains a critical issue, with threats such as hacking, malware, and phishing threatening the security of individuals and organizations alike.

Digital Divide: The “digital divide” is the gap between individuals who have access to modern Information and Communication Technology (ICT) resources, such as the Internet and digital devices, and those who lack such access. This disparity leads to unequal opportunities and access to information, as not everyone can equally benefit from digital advancements.

Misinformation: The proliferation of misinformation and fake news canhave serious societal consequences.

Addressing these challenges requires ongoing efforts in policy, education, and technological innovation to promote a safe, inclusive, and trustworthy online environment.

2.6 REGULATION IN CYBERSPACE

Cyberspace, spanning the globe, operates without a definitive framework as it lacks ownership or control by any singular entity, individual, or government. Consequently, the challenge of regulating cyberspace is steadily emerging.

Regulations in cyberspace are crucial for safeguarding users and organizations from cyber threats. These regulations are established by various governmental and international bodies to ensure the security of personal data, maintain privacy, and protect the digital environment. Governments and international entities collaborate to formulate policies capable of addressing evolving cyber threats effectively.

Each country maintains distinct laws governing physical business transactions, which differ significantly from those governing online transactions. As technology advances, there is a growing imperative to regulate human behaviour in cyberspace. Cyber laws have been enacted to promote responsible technology use. Any activity that infringes upon the rights of individuals within cyberspace constitutes a cyber violation and is subject to punishment under these laws.

Regulatory Frameworks

Cyber threats often cross borders, making international cooperation crucial. For instance,

- General Data Protection Regulation (GDPR) is the strictest privacy and security law globally. Although created by the European Union (EU), it applies to any organization worldwide that targets or collects data from people in the European Union.
- The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides guidelines to improve cybersecurity risk management.
- India has several regulatory frameworks to protect critical information infrastructure, enhance cybersecurity, and safeguard personal data. Amendments to the Information Technology Act, 2000, introduced key cybersecurity provisions.

As cyberspace becomes more integral to our lives, the need for regulation to protect individuals, businesses, and society from cyber threats and misuse becomes increasingly critical.It is necessary to regulate the cyberspace, because of

- **Rising Cyber-attacks**
- **Increased Digital Usage**
- **Impact on Businesses**
- **Impact on Individuals**

Let us discuss these attacks very briefly.

1. **Rising Cyber-attacks:** Cyber-attacks and cyber-crime have become rampant. In India, like in many other countries, the incidence of cyber-crime is escalating rapidly. As technology becomes integral to daily life, people increasingly depend on the Internet for activities such as shopping, gaming, online education, social networking, and work. Cyber criminals exploit the speed, convenience, and anonymity provided by the Internet to commit various crimes such as phishing, credit card fraud, bank robbery, and distribution of viruses.

   The National Crime Records Bureau (NCRB) in India plays a crucial role in collecting, analyzing, and disseminating information related to crime and criminal justice. The NCRB collects data on various types of crimes reported across the country. This includes both conventional crimes like theft, murder, and assault, as well as

modern crimes such as cybercrime and economic offenses. The bureau maintains a centralized national crime database, which serves as a repository of crime-related information.In recent years, the NCRB has expanded its focus to include cybercrime monitoring and reporting. It tracks and reports on incidents of cybercrime, including data breaches, online fraud, cyber-attacks, and other digital offenses.

2. **Increased Digital Usage:**Many sectors, like financial services, banking, energy, manufacturing, and nuclear power plants, are quickly becoming digital. People now spend a lot of time online for work, education, entertainment, and business. The Internet connects people globally, allowing millions to share and access information every day. However, digital data is often stored in different places, and users might not know where their information is kept or which laws apply. This anonymity lets people do things online without revealing their identity, which can lead to misuse and requires oversight and regulation.
3. **Impact on Businesses:**The Internet's fast and efficient data transmission has transformed global trade. It enables paperless transactions and improves efficiency. Online banking and digital payment platforms like Google Pay and PhonePe have made financial transactions easy and common.
4. **Impact on Individuals:**The Internet allows people to share and receive digital content like photos, music, videos, and eBooks. Children are becoming skilled at using smartphones and laptops for games and videos. The digital world gives shy individuals a place to express themselves, but it also has risks. Personal information shared on social media can be misused, leading to serious problems. Children and elderly people, who may not recognize online dangers, are especially at risk. Therefore, protecting personal information and financial accounts online is just as important as safeguarding physical assets.

Awareness, education, and stringent laws are essential to foster a safe and secure digital environment for all users.

2.7 CONCEPT OF CYBER SECURITY

For communication over the Internet, a variety of software, hardware, communication channels, and mediums are interconnected to facilitate the sharing and exchange of information. It's crucial to have security mechanisms in place to protect against unauthorized access to information across these interconnected systems. Cybersecurity is the practice of safeguarding these systems from cyber threats.

Modern technology has significantly altered people's lifestyles, leading to increased use of technology for financial transactions and shopping within cyberspace. With the widespread growth of social media, there has been a corresponding rise in online crime, or cybercrime. Just as we take precautions in the physical world - locking our homes, cars, and offices, and storing valuable documents in bank safety deposit boxes- we must also protect ourselves in the digital realm. Despite our reliance on the Internet for work and social life through email and the World Wide Web, we often neglect online security. It's a mistake to assume that the virtual world is safer or more benign than the real world. We must prioritize securing our data and information when sharing online in this age of new technology.

Information security has become a major challenge today. Cybersecurity involves a range of technologies, processes, and measures designed to reduce the risk of cyber-attacks and protect individuals and organizations from computer-based threats. Cyber-attacks can cause significant damage to computer systems or result in the theft of important information. Issues such as money laundering and identity theft in cyberspace have highlighted the need for enhanced cybersecurity. Cyber-crime, where computers or networks are used as tools or targets for committing crimes, is a growing concern. Governments and businesses are taking various steps to combat this form of crime. To protect users, governments have introduced several cyber laws to ensure technology is used responsibly and not misused. In the upcoming units of this course, we will delve into key concepts such as cyber-crimes and cyber laws.

2.7.1 Issues and Challenges of Cyber Security

Cyber security has become a vital issue for everyone, including individuals, businesses, and governments. As more personal and sensitive informationlike photos, videos, travel details, and financial datais shared online, ensuring its safety is crucial. The growing dependence on digital technologies, especially after the pandemic, has increased the frequency and severity of cyberattacks. This increase in online threats has made cybersecurity a top priority.

In this section, we will discuss some of the important cybersecurity challenges that many industries and organizations, individuals are facing today.

- Ransomware Attacks
- Cloud Attacks
- IoT Attacks
- Phishing Attacks
- Cryptocurrency Attacks
- Mobile Banking Malware
- AI Attacks
- Insider Attacks
- Social Engineering Attack
- Man-in-the-Middle Attack

Ransomware Attack: Ransomware is one of the biggest cyber security challenges. Ransomware is a type of malicious software (malware)designed to deny users access to their computer system including files and protected data until ransom amount is reimbursed to the hackers. It threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker.In the year 2021-2022, due to the increased digital usage after the Covid pandemic, there were a huge number of ransomware attacks.Over 20% of cyberattacks in 2021 were categorized as ransomware. Some percentage of ransomware attacks were unreported.

Cloud Attacks: Cloud computing has become increasingly popular in recent years, revolutionizing data storage from physical servers to virtual platforms. Initially used for backup storage, cloud computing has evolved into a versatile computing platform transforming how organizations manage, store, and share information. However, weaknesses in cloud security, such as inadequate data encryption, weak authentication methods, and improper system configurations, pose significant risks. Attacks on cloud platforms have been on the rise, including Distributed Denial-of-Service (DDoS) attacks, which flood servers and networks with traffic, disrupting services and hindering legitimate user access. For instance, Azure Networking reported more DDoS attacks in the first half of 2021 compared to the previous year, highlighting growing security challenges in cloud environments.

IoT Attacks: The Internet of Things (IoT) connects a vast array of devices, from smart home appliances to industrial machinery, to the internet. This connectivity brings convenience and efficiency but also introduces new security vulnerabilities. IoT devices often lack robust security features, making them attractive targets for cybercriminals. Attacks on IoT devices can lead to data breaches, loss of control over devices, and even physical damage in critical infrastructure.

Phishing Attacks: Phishing remains one of the most common and effective cyberattack methods. Attackers use deceptive emails, messages, or websites to trick individuals into revealing sensitive information such as passwords, credit card numbers, or personal data. Phishing attacks can lead to identity theft, financial loss, and unauthorized access to systems.

Cryptocurrency Attacks: The rise of cryptocurrencies and blockchain technology has introduced new security challenges. Cybercriminals target cryptocurrency exchanges and wallets, exploiting vulnerabilities to steal digital assets.

Mobile Banking Malware: With the increasing use of mobile devices for banking and financial transactions, mobile banking malware has become a significant threat. These malicious programs target mobile apps to steal sensitive information, intercept communications, or manipulate transactions. Users can unknowingly download malware through malicious apps or links, leading to substantial financial losses.

AI Attacks: Artificial Intelligence (AI) is transforming various industries, but it also presents new cybersecurity challenges. Attackers can use AI to develop sophisticated malware, automate attacks, and identify vulnerabilities. Conversely, AI can also enhance security by improving threat detection and response. The dual-use nature of AI requires careful management to prevent misuse by cybercriminals.

Insider Attacks: Insider threats come from employees, contractors, or business partners who have access to an organization's systems and data. These individuals can intentionally or unintentionally cause significant damage by leaking sensitive information, sabotaging systems, or facilitating external attacks. Insider attacks are challenging to detect and prevent due to the trusted status of the individuals involved.

Social Engineering Attacks: Social engineering exploits human psychology to manipulate individuals into performing actions or divulging confidential information. Techniques such as pretexting, baiting, and tailgating can be used to gain unauthorized access to systems or data. Social engineering attacks are particularly effective because they bypass technical defenses by targeting the human element.

The Man-in-the-Middle Attack: In a Man-in-the-Middle (MitM) attack, the attacker secretly intercepts and relays communications between two parties. This type of attack can occur over unsecure networks, allowing the attacker to eavesdrop, modify, or steal information being exchanged. Man-in-the-Middle Attack pose significant risks to financial transactions, communications, and sensitive data.

There are certain factors on which these challenges depend on. Some of them are:

- **No Procedural Rules:** The lack of standardized procedures and regulations for cybersecurity across industries and regions leads to inconsistent protection levels and gaps in defences.
- **Shortage of Technical Staff:** There is a global shortage of skilled cybersecurity professionals, making it difficult for organizations to effectively defend against cyber threats.
- **Lack of Infrastructure:** Insufficient investment in cybersecurity infrastructure and laboratories hinders the development and testing of robust security measures.
- **Need for Localization:** Different regions have unique cybersecurity requirements and threats. Localized strategies and solutions are necessary to address these specific challenges effectively.

Addressing these cybersecurity challenges requires a comprehensive approach that includes robust technical defences, regular training and awareness programs, investment in cybersecurity infrastructure, and the development of standardized procedures and regulations.



CHECK YOUR PROGRESS

Q1. Choose the correct option:

i. The first network that planted the seeds of Internet was:

a) NFSNET b) ARPANET

c) Telnet d) ARPA

ii. The communication protocols used by Internet is

a) TCP/IP b) HTTP

c) SMTP d) WWW

iii. To access the Internet, the user needs to be connected to an

a) Internet Service Provider b) Server

c) DNS d) None of these

iv. Internet is a

a) complex system b) dynamic system

b) decentralized system d) all of these.

Q2. What is ARPANET?

Q3. Fill in the blanks:

i. _____ are large-scale fiber optic cables laid on the ocean floor, connecting continents and enabling global data transfer.

ii. _____is foundational for the smooth operation of the Internet, ensuring reliable and secure communication.

iii. _____ is the core protocol for data communication on the World Wide Web, with _____ being its secure version that adds an encryption mechanism.

iv. _____ provide critical physical space and power required for data processing and storage, forming the backbone of Internet infrastructure.

v. Ransomware is a type of malicious software designed to deny users access to their computer system until _____ is paid to the hackers.

vi. Weaknesses in cloud security include inadequate _____, weak authentication methods, and improper system configurations.

vii. Phishing attacks aim to trick individuals into revealing sensitive information such as _____ or personal data.

viii. Cybercriminals exploit vulnerabilities in cryptocurrency exchanges and wallets to steal _____ assets.

ix. In a Man-in-the-Middle attack, the attacker secretly intercepts and relays _____ between two part



2.8 LET US SUM UP

- The Internet is a global network connecting computers and devices worldwide.

- It enables communication and information sharing through standardized protocols.
- ARPANET, developed by the U.S. Department of Defense in the 1960s, aimed to create a resilient communication system.
- Adoption of TCP/IP protocols in the 1970s expanded ARPANET's capabilities.
- By the early 1980s, ARPANET connected academic and research institutions globally.
- Tim Berners-Lee's invention of the World Wide Web in 1989 revolutionized the Internet, facilitating commercial use and global network connectivity.
- Internet infrastructure includes physical hardware, data transfer protocols (e.g., TCP/IP, HTTP), and data centres.
- These components ensure efficient, reliable, and secure data transmission, complying with regulatory standards for data protection.
- The Internet Society promotes global information exchange and supports the Internet's development as a global technical infrastructure.
- It aims to enrich people's lives through universal Internet access and usage.
- Increasing reliance on digital technologies heightens cybersecurity concerns for individuals, businesses, and governments.
- Key challenges include ransomware, cloud attacks, IoT vulnerabilities, phishing, cryptocurrency attacks, mobile banking malware, AI threats, insider attacks, and social engineering.
- Addressing these threats requires robust defenses, skilled cybersecurity professionals, adequate infrastructure, and standardized regulations to mitigate risks effectively.



2.9 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q. No. 1:

Q1. i. b) ARPANET ii. a) TCP/IP

iii. a) Internet Service Provider iv. d) all of these

Answer to Q. No. 2: TheAdvanced Research Projects Agency Network (ARPANET) is the precursor to the Internet. It was established by the Advanced Research Projects Agency (ARPA) of the United States Department of Defense in the late 60s and early 70s as an experiment inWAN to connect together computers that were running different systems so that people at one location could use computing resources from another location.ARPANETwas one of the first networks to implement the TCP/IP protocol suite.

Answer to Q. No. 3:

i. Undersea cables
ii. Transmission Control Protocol/Internet Protocol (TCP/IP)
iii. Hypertext Transfer Protocol (HTTP), HTTPS
iv. Data centres
v. Ransom
vi. data encryption
vii. passwords
viii. digital
ix. communications
x. malware



2.10 FURTHER READING

1) Forouzan, B., &Fegan, S. (2006). Data Communication and Networking, Special Indian Edition *Tata McGraw Hill Education Private Limited*.
2) Internet Society Mission and Vision - Internet Society
3) https://www.legalserviceindia.com/legal/article-2548-need-of-regulation-in-cyberspace.html
4) https://legaldesire.com/laws-applicable-in-cyberspace-in-india/
5) https://increditools.com/ransomware-statistics/
6) https://www.thesagenext.com/blog/emerging-cybersecurity-challenges

7) https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050

8) https://gdpr.eu/

9) https://www.researchgate.net/publication/347373943_Cyber_Security_Challenges_and_its_Emerging_Trends_on_Latest_Technologies



2.11 MODEL QUESTIONS

Q1. What is the Internet?

Q2. What is cyber security?

Q3. What is mean by digital divide?

Q4. What does “cyberspace” mean?

Q5. How does real space differ from cyberspace?

Q6. Why is the Internet referred to as a network of networks?

Q7. What are some negative impacts of the Internet on society, and how can they be mitigated?

Q8. What is the mission and vision of the Internet Society?

Q9. What are five activities conducted by the Internet Society?

Q10. What are the key issues and challenges in cyber security? Describe.

Q11. Why are regulations necessary for cyberspace?

Q12. How has the advent of the Internet transformed communication and connectivity globally?

Q13. Discuss briefly the impact of ransomware attacks on individuals and organizations.

Q14. Explain how the Internet has revolutionized communication and connectivity globally.

*** ***** ***

UNIT 3 –CYBER CRIME (PART I)

UNIT STRUCTURE

3.1 Learning Objectives

3.2 Introduction

3.3 Cyber Crime

3.4 Classification of Cyber Crimes

3.5 Common Cyber Crimes

- 3.5.1 Cyber Crimes Targeting Computers and Mobile Devices
- 3.5.2 Cyber Crimes Against Individuals
- 3.5.3 Cyber Crimes Against Women and Children

3.6 Let Us Sum Up

3.7 Answers to Check Your Progress

3.8 Further Reading

3.9 Model Questions

3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- define cybercrime
- classify different types of cybercrimes
- list common cybercrimes
- describe cybercrimes targeting computers and mobiles
- describe cybercrimes against individuals
- describe cybercrimes against women and children

3.2 INTRODUCTION

In the previous unit, we have learnt about internet and concepts related to internet like internet infrastructure for data transfer and governance. We have also learnt about regulation of cyberspace, concept of cyber security, its issues and its challenges in detail. In this unit we will be introduced to the different types of cybercrime. We will also learn about the categories of cybercrime. Cybercrimes targeting computers and mobiles are discussed in detail in this unit. In addition to this, cybercrimes against individuals and

specially against women and children are also covered in detail in this unit. In the next unit, we will learn about the different types of financial fraud and social engineering attacks. We will also learn about the different types of malware in the next unit.

3.3 CYBER CRIME

Computers and electronic devices have become integral to our daily lives, facilitating a range of activities from communication and entertainment to banking and education. This widespread adoption has simultaneously spurred the exponential growth of internet use, connecting billions of people globally. The internet and digital technology have undoubtedly simplified many aspects of life, however, this digital revolution has also led to the emergence of a new category of crime—cybercrime.

As per the Indian National Cyber Crime Reporting Portal, cybercrime is defined as:

"Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime."

Cybercrime can be defined as any crime that is performed using a computer and network either as a tool or as a target. This definition underscores the dual role that technology can play in cybercrime—as both a medium for committing traditional crimes (like fraud or harassment) and a target in itself (like in the case of hacking).

3.4 CLASSIFICATION OF CYBER CRIMES

There are a lot of cybercrimes and depending on the type of category it can be classified into different groups. In general, one of the common classifications for cybercrimes is based on the target of the cybercrimes.

The following are the categories of cybercrimes based on their target:

1. **Crimes against Institution and Government:** When cybercriminals hack into the computer systems or are able to install malware into the computer systems of a target organization or nation then these cybercrimes are considered to be crimes against the organizations or government and the country. Some

of the examples of crimes against government are cyber terrorism, installing spyware etc.

2. **Crimes against Individuals:** When cybercriminals target an individual by hacking into their computer systems or by installing malware into their systems then these cybercrimes are considered to be crimes against individuals. Some of the examples of these category of crimes includes financial frauds, hacking of computer or mobile devices etc.
3. **Crimes against Property:** When cybercriminals target intellectual property and digital assets, infringing on rights and causing significant financial losses then these cybercrimes are considered to be crimes against property.
4. **Crimes against Society:** Crimes against society are large-scale cybercrimes that aim to disrupt societal norms and endanger public welfare. These include activities like using computer systems for human trafficking, spreading child pornography and digital forgery of currency.

Cybercrimes can also be classified based on how computers are used in the commission of the crime into two categories:

- **Targeted at Computers:** In this category, the computer itself is the primary target. Examples for this category include hacking, malware attacks and denial-of-service attacks.
- **Using Computers as Tools:** In this category, computers are used as instruments to facilitate the crime. Examples for this category include cyberstalking, cyberbullying, and various forms of online fraud and identity theft.



CHECK YOUR PROGRESS

Q1. Define cybercrime.

Q2. What are the categories of cybercrime based on target?

3.5 COMMON CYBER CRIMES

In this section, we will look into some of the common cybercrimes. These common cybercrimes are classified intofollowing categories:

1. Cyber Crime targeting Computers and Mobile Devices
2. Cyber Crime against Individuals
3. Cyber Crime against Women and Children

3.5.1 Cyber Crime Targeting Computers and Mobiles Devices

Let us look at the different types of cybercrimes that target computers and mobile devices.

1. Hacking

Hacking is one of the most common cybercrimes. Hacking involves getting into the computer system or mobile devices of another person without permission and by using illicit means. Hacking can also be defined as an illegal intrusion into another person's computer system or network. It can also be defined as the activity of finding vulnerabilities in a computer system and the computer network and to exploit these vulnerabilities and gain access to the data and device.

Hackers, the criminals that hack the system maybe an individual, or belong to a team or an organization. Hackers are generally categorized into three categories:

White hat hackers: White hat hackers are ethical hackers who are typically employed by organizations to test the security of their systems. They try to protect the system by finding flaws in the system so that these flaws can be fixed. White hat hackers are also called as ethical hackers since they hack with the objective of protecting the system from future hacks.

Black hat hackers: Black hat hackers are the opposite of white hat hackers. They hack into computer systems and networks illegally, without the permission of the system owners. Their primary objective is to exploit vulnerabilities for personal gain, which can include financial theft, data breaches, and spreading malware.

Grey hat hackers: Grey hat hackers are hackers who hack into computer systems and network without the permission of the owner of the systems but do not do so with ill intent or for financial gain. Most often they hack into the system to test the security and protection levels of the systems and inform the administrator of those systems about the vulnerabilities of the system.

2. Software Piracy

Software piracy can be defined as the illegal copying and illegal distribution of copyrighted software. When a copyrighted software is illegally distributed, the owners of the software do not get the revenue for that software. This in turn may also lead to an increase of the price of the software for legitimate users. To combat this, many software companies run “anti-piracy” campaigns or most software’s include an End User License Agreement (EULA) which users must agree to, specifying the terms of software use to prevent piracy.

Let us look at the different categories of software piracy [4]:

- **Softlifting:** Softlifting occurs when a program is shared with someone who is not authorized to use it under the license agreement. A common example is purchasing a single copy of software and installing it on multiple computers without additional licenses.
- **OEM Unbundling:**OEM unbundling involves the illegal separation and sale of software that was intended to be sold only with specific hardware or as part of a software bundle. This practice violates licensing agreements and can dilute the intended user experience.
- **Internet Piracy:** Internet piracy, or online piracy, involves the unauthorized distribution of copyrighted software over the internet. This can include hosting pirated software on websites, sharing it through peer-to-peer networks, or providing direct download links.
- **Software Counterfeiting:** Software counterfeiting is the illegal duplication, distribution, and sale of copyrighted software. Products like Microsoft’s Windows and Office are commonly counterfeited due to their high demand.

- **Hard Disk Loading**: Hard disk loading occurs when hardware dealers install unauthorized copies of software onto computers they sell, making their products more attractive to buyers.
- **Renting:**Renting involves the temporary distribution of licensed software to users who do not have the proper license to use it. This practice violates the terms of most software licenses, which typically prohibit renting, leasing, or lending the software.

3.5.2 Cyber Crime AgainstIndividuals

1. Digital Forgery:

Forgery is the process of falsely making and altering a document or even possessing a forged document. Digital forgery can be defined as the process of forging a document using digital means. Some of the common digital forgery examples include signatures, counterfeit currency notes, mark sheets etc. Digital technologies like printers, copiers and image scanners are used by cybercriminals to make forged documents like identity proofs, passports etc.

Let us look at some of the different types of digital forgery:

- **Document Forgery:**Document forgery involves the digital manipulation or replication of legal documents. Common examples include forged mark sheets, certificates, and revenue stamps.
- **Counterfeit Money Forgery:**Counterfeit money forgery involves the digital replication of currency notes. Criminals use high-resolution scanners and printers to produce fake currency that resembles genuine legal tender.
- **Digital Signature Forgery:** Digital signature forgery involves the unauthorized replication of an individual's signature using digital means. This can be done by scanning a genuine signature and then copying it onto other documents, or by using software to create a signature that closely resembles the original.
- **Art Forgery:**Art forgery in the digital realm includes the replication of artworks or the falsification of an artist's signature on a piece

of art. Cybercriminals may use digital tools to create convincing replicas of famous paintings or to add a well-known artist's signature to a lesser-known or fake artwork to increase its value.

2. Cyber Terrorism:

Cyber terrorism can be defined as an act of terrorism that is done using computer and networks. It is mainly done by cyberterrorists for political or ideological gains and to threaten and intimidate the victims. Cyberterrorism may result in loss of resources, properties and many a times even human life. Cyberterrorists also try to cause failure of government services by targeting these services specifically. For example, the medical services, electric and solar power plants, air and rail traffic control systems, police and military services, any essential services etc. are most often the popular targets of cyberterrorists. One of the earliest known instances of cyber terrorism occurred in 1998 when ethnic Tamil guerrillas launched an attack against Sri Lankan embassies by sending 800 emails per day over a two-week period.



LET US KNOW

Cyber warfare can be defined as the actions against a nation or state to damage, disrupt services of the target nation using computer systems and network. This could be done for many objectives like economic warfare, espionage, sabotage, propaganda and manipulation.

3. Cyber Defamation:

Defamation can be defined as the act of damaging somebody's reputation by saying or writing bad or false things about them. When a person is defamed in cyber space it is called as cyber defamation. Cyber defamation can be defined as defamation that is done using computer systems and internet. For example, when a person publishes defamatory matter about someone on a website it is cyber defamation. Defamation can occur both orally (slander) and in written form (libel).

There are two ways in handling cyber defamation.

1. **Cease and desist letter:** In cases where there is **no serious grudge** against the person, then a cease and desist letter can be used for removing the defamatory messages from the digital media. This letter demands the removal of the defamatory content and cessation of further defamatory actions.
2. **Legal recourse:** When the defamation is done with serious intent to harm, then legal recourse may be necessary. Laws can be utilized to punish the offenders.

Cyber defamation not only damages the reputation of the individual but can also negatively impact their family, organization, and even the nation, particularly if the individual holds a prominent position. Let us look at the two types of liability for defamation in India. In the first category, the persons who have written or published the defamatory material are liable. In the second category, the internet service providers and similar service providers who had authorized the publication of defamatory material are held liable.

3.5.3 Cyber Crime Against Women and Children

Cybercrimes targeting women and children have become an alarming issue in the digital age. The rise of digital devices and online platforms has created new opportunities for criminals to target vulnerable individuals, often with devastating consequences. Let us look at the different types of cybercrimes that are specifically committed against women and children.

1. Cyber Stalking:

Stalking is the act of harassing the victim. Stalking includes various acts like following the victim, making harassing phone calls, vandalizing the property of the victim, leaving written messages or objects for the victim to find etc. Cyberstalking can be defined as the act of stalking that is carried out using internet and online technologies. Although any individual can be a victim of cyberstalking, women are more generally the targets for cyberstalking.

In many cases of cyber stalking, the victim is being harassed by the stalker by sending repeated online messages and emails. The cybercriminals also harass the victims by posting messages in groups and discussion forums. The criminals try to track the daily routine of the victim with the help of social media applications like Facebook, Instagram, Twitter etc. Most of the victims share their daily routine, places they visited and events they participated in along with live location on social media nowadays. This makes is extremely easy for cyber stalkers to stalk the victim both online and offline. Many times, the online stalkers also resort to offline stalking in addition to online stalking.

2. Cyber Harassment:

Cyber harassment is the use the internet andelectronic means to harass, control, manipulate or habitually disparage a child, adult, business or group without a direct or implied threat of physical harm. Cyber harassment requires the use of ICT and maybe verbal, sexual, emotional or social abuse of a person, group or organization. The cyber harasser's primary goal is to exert power and control over the targeted victim.

3. Cyber Bullying:

Cyberbullying, the act of bullying through online methods or electronic means, particularly among teenagers and children. It can be defined as "the activity of using messages on social media, emails, text messages, etc. to frighten or upset somebody."Cyberbullying is also known as online bullying.

After and during COVID-19 pandemic, students shifted to online learning increasing screen time and their dependence on digital platforms for education and social interaction which have made them vulnerable to cyberbullies.Often times, the victims are trolled on online community forums for online gaming or other popular social media sites to bring about a reaction or for simply the enjoyment of the cyberbully. In most cases, the victims who are cyberbullied may also face other kinds of bullying in the offline world, sometimes even physically. Victims often suffer from low self-esteem, heightened levels

of stress, and in severe cases, depression.

4. Online Predation:

Online predation is a form of cybercrime targeting vulnerable individuals, particularly children, through various online platforms. Predators often exploit the anonymity and accessibility of the internet to groom and manipulate their victims for sexual exploitation or other harmful purposes. They may use social media, chat rooms, online gaming platforms, or messaging apps to establish relationships with minors under false pretenses, gradually gaining their trust and confidence. This manipulation can involve deceptive tactics, such as pretending to be someone the victim knows or offering attention, gifts, or promises of affection. Once trust is established, predators may escalate their behavior, coercing victims into engaging in sexual activities, sharing explicit images or videos, or meeting in person.

5. Cyber Pornography:

Cyber pornography refers to the publishing, distributing, or designing of pornographic content through cyberspace. Pornographic content includes any videos, pictures, or movies that contain sexually explicit acts considered indecent by public standards. The spread of the internet and digital technologies has made access to and distribution of pornography easier and more widespread than ever before, raising numerous social, ethical, and legal issues.

6.Sextortion:

The term “sextortion” is the blending of two words “sex” and “extortion”. Sextortion is a cybercrime where criminals threaten the victim and extort sexual favors in return from the victim. Sextortion in many cases involves the threatening to share intimate details, sexual images or videos of an individual online if the demands are not fulfilled. In most cases, the criminals demand sexual favors or money in return. Although anyone can be a victim of sextortion, often women and children are targeted in sextortion cases.

7. AI Generated Threats: Deep Fakes

One of the most concerning developments in recent years is the rise of deep fakes, a form of synthetic media generated using deep

learning techniques. Deep fakes involve creating highly realistic, but entirely fabricated, audio, images, or video content that can be used to deceive or manipulate individuals. Deep fake technology utilizes neural networks, particularly generative adversarial networks (GANs), to generate or manipulate digital content. These networks are trained on large datasets of images, videos, or audio recordings to learn patterns and features, enabling them to create highly realistic simulations of human faces, voices, and behaviors.With the ability to create convincing fake videos or audio recordings of individuals, criminals can manipulate public opinion, spread disinformation, or perpetrate various forms of fraud and social engineering attacks.

8. Cyber Slavery:

Cyber slavery, also known as online exploitation or digital slavery, refers to the use of digital technology, particularly the internet, to exploit individuals for forced labour, sexual exploitation, or other forms of modern slavery. One of the most prevalent forms of cyber slavery is online human trafficking. Traffickers use the anonymity and reach of the internet to recruit and exploit vulnerable individuals, particularly women and children, for commercial sexual exploitation or forced labour. They lure victims through false promises of employment, education, or romantic relationships, only to subject them to coercion, manipulation, and violence.

9. Cyber Kidnapping:

Cyber kidnapping, also known as virtual kidnapping or online kidnapping, is a form of extortion where criminals use deception and psychological manipulation to exploit victims and extract ransom money. Unlike traditional kidnapping, which involves physically abducting a person, cyber kidnapping occurs entirely online and relies on threats and coercion to achieve its objectives. In a typical cyber kidnapping scheme, perpetrators use various methods to target their victims, such as phishing emails, social engineering tactics, or malware infections. They often prey on individuals who are vulnerable or easily deceived, such as parents with children or elderly individuals living alone.



CHECK YOUR PROGRESS

Q3. Who are white, black and grey hat hackers?

Q4. Define cyberstalking.

Q5. Define online predation.

Q6. What are deep fakes?



3.6 LET US SUM UP

- Cybercrime can be defined as any crime that is performed using a computer and network either as a tool or as a target.
- Hacking can also be defined as an illegal intrusion into another person's computer system or network.
- Digital forgery can be defined as the process of forging a document using digital means.
- Software piracy can be defined as the illegal copying and illegal distribution of copyrighted software.
- Cyber terrorism can be defined as an act of terrorism that is done using computer and networks.
- Cyber defamation can be defined as defamation that is done using computer systems and internet.
- Cyberstalking can be defined as the act of stalking that is carried out using internet and online technologies.
- Cyber harassment is the use the internet and electronic means to harass, control, manipulate or habitually disparage a child, adult, business or group without a direct or implied threat of physical harm.
- Cyberbullying is the act of bullying done through online methods or electronic means.
- Cyber pornography means the publishing, distributing or designing pornography by using cyberspace.
- Online predation is a form of cybercrime targeting vulnerable individuals, particularly children, through various online platforms.

- Sextortion is a cybercrime where criminals threaten the victim and extort sexual favors in return from the victim.
- Deep fakes involve creating highly realistic, but entirely fabricated, audio, images, or video content that can be used to deceive or manipulate individuals.
- Cyber slavery, also known as online exploitation or digital slavery, refers to the use of digital technology, particularly the internet, to exploit individuals for forced labour, sexual exploitation, or other forms of modern slavery.
- Cyber kidnapping, also known as virtual kidnapping or online kidnapping, is a form of extortion where criminals use deception and psychological manipulation to exploit victims and extract ransom money.



3.7 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q1: Cybercrime is defined as any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of crime.

Answer to Q2: The categories of cybercrime based on target are:

a) Crimes against institution or government
b) Crimes against individuals
c) Crimes against property
d) Crimes against society

Answer to Q3: Hackers who are usually employed by the target system's owner to find vulnerabilities in their own computer systems and network are called white hat hackers. Hackers who hack into computer systems and network illegally are called black hat hackers. Grey hat hackers are hackers who hack into computer systems and network without the permission of the owner of the systems but do not do so with ill intent or for financial gain.

Answer to Q4: Cyberstalking can be defined as the act of stalking that is carried out using internet and online technologies. Cyberstalking can also be defined as the use of the Internet or other electronic means to intimidate and harass a victim.

Answer to Q5: Online predation is a form of cybercrime targeting vulnerable individuals, particularly children, through various online platforms.

Answer to Q6: Deep fakes involve creating highly realistic, but entirely fabricated, audio, images, or video content that can be used to deceive or manipulate individuals.



3.8 FURTHER READING

1) https://en.wikiversity.org/wiki/Digital_Media_Concepts/Cyber_Crimes
2) https://www.javatpoint.com/types-of-hackers
3) https://www.legalservicesindia.com/article/365/Historical-Perspective-of-Terrorism-&-Cyber-Terrorism.html
4) https://blog.ccasociety.com/cyber-defamation/
5) https://cs.stanford.edu/people/eroberts/cs181/projects/1999-00/software-piracy/types.html
6) https://ipredator.co/cyber-harassment/
7) https://en.wikipedia.org/wiki/Cyberbullying
8) https://www.oxfordlearnersdictionaries.com/definition/english/cyberbullying?q=cyberbullying
9) https://blog.ipleaders.in/cyber-pornography/



3.9 MODEL QUESTIONS

Q1. Define cybercrime. Describe the categories of cybercrime.

Q2. Describe the cybercrimes that are committed against women and children.

Q3. Describe the cybercrimes targeting computers and mobiles.

Q4. Explain the different types of software piracy.

Q5. Explain the different types of digital forgery.

Q6. Explain how cyberterrorism and cyberwarfare are used to attack a country.

Q7. Define hacking. What are the different types of hacking?

Q8. How are cyber harassment and cyber bullying used to threaten women and children?

Q9. Explain how deep fakes are used to target women.

Q10. What are cyber slavery and cyber kidnapping?

*** ***** ***

UNIT 4 –CYBER CRIME (Part II)

UNIT STRUCTURE

4.1 Learning Objectives

4.2 Introduction

4.3 Financial Frauds

- 4.3.1 Identity Fraud
- 4.3.2 Investment Fraud
- 4.3.3 Mass Marketing Fraud
- 4.3.4 Internet Banking Fraud
- 4.3.5 UPI Payment Gateway Fraud
- 4.3.6 ATM Cloning
- 4.3.7 SIM Cloning

4.4 Social Engineering Attacks

- 4.4.1 Phishing
- 4.4.2 Baiting
- 4.4.3 Water Holing
- 4.4.4 Pretexting
- 4.4.5 Quid Pro Quo
- 4.4.6 Tailgating
- 4.4.7 Impersonation

4.5 Malware

4.6 Zero Day Attack

4.7 Zero Click Attack

4.8 Let Us Sum Up

4.9 Answers to Check Your Progress

4.10 Further Reading

4.11 Model Questions

4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- define financial fraud and social engineering attack

- describe the different financial frauds
- describe various social engineering attacks
- define malware and its various categories
- describe how zero-day attack works
- define zero click attack

4.2 INTRODUCTION

In the previous unit, we have learnt about cybercrime and delved into the different categories of cybercrimes. We have already learnt about the many different types of cybercrimes that target individuals and specificallytarget women and children like cyber stalking, cyber bullying etc. Similarly, we have also learnt about the different types of cybercrimes that target our computers and mobile phones like hacking.

In this unit we will learn about the different financial frauds. We will also learn about the different social engineering attacks. Different types of malware are also discussed in detail in this unit. Cybercrimes like zero-day attack and zero click attacks are also discussed in this unit. In the next unit we will learn about the cyber laws that can be used to deal with different cybercrimes.

4.3 FINANCIAL FRAUDS

Financial fraud occurs when individuals or organizations through deceptive, misleading and illegal practices deprives us of our money or harm our financial health. We need to understand the various types of financial frauds so that we can protect ourselves from these crimes.

Some of the ways by which financial fraud is done are as follows:

- Identity Fraud
- Investment Fraud
- Mass Marketing Fraud
- Internet Banking Fraud
- UPI Payment Gateway Fraud

- ATM cloning
- SIM cloning

Let us look at each of these financial fraud in detail.

4.3.1 Identity Fraud

Identity fraudis a crime that occurs when a criminal steals or uses another person's personal information without their permission to commit a financial fraud. The criminal generally uses the victim's identity to obtain money, loans or any other financial benefit.

Mostly the information that is stolen are financial in nature like bank account number and details, credit cards, debit cards, digital payments information, ATM PINs etc. to make fraudulent withdrawals from the victim's bank account. The stolen information can also be unique or identifying personal information like PAN, Aadhar number etc. This information may beused to open new bank or credit card accounts and make the victim liable for all the charges. Identity fraud may lead to low CIBIL score or credit score which hampers the financial health of the victim.

4.3.2 Investment Fraud

Investment fraud is a crime that occurs when criminalsconvinces people to invest in schemes that are have zero potential or sometimes don't even exist. The criminal generally sells the victim these schemes with false and misleading information of great returns. In most cases, once the investment has been made, the criminal ceases contact with the victim.

Some of the common investment frauds are:

- **Ponzi Scheme:**In this type of investment fraud, criminals collect money from new investors to pay existing investors. The scheme ends when no new investors join and the schemers keep the remaining money by not paying return to the old investors.
- **Pyramid Schemes:** Pyramid schemes rely on the recruitment

of new participants to generate returns for earlier investors, with the scheme eventually failing as the pool of potential recruits is exhausted.

- **Advance Fee Fraud:** In this scheme, victims are promised large sums of money or other high-value items in return for an advance payment. The initial fee is often explained as a processing fee, tax, or some other pretext.
- **Pump and Dump Fraud:** Investors nowadays use internet and social media to influence decision on which stocks to buy and where to invest their money by making some stocks look more profitable. This involves inflating the price of a stock through false or misleading statements.

4.3.3 Mass Marketing Fraud

Mass marketing fraud is a type of financial crime that targets a large number of potential victims through mass communication channels, such as emails, social media, telemarketing, online advertisements etc.

Some of the common types of mass marketing fraud are:

- **Lottery Fraud:** In this type of fraud, the victims are informed that they have won a lottery they never entered. To claim the prize, they are instructed to pay fees or taxes upfront but once the payment is made, the prize never materializes.
- **Romance Scams:** In this scam, fraudsters create fake profiles on dating sites or social media to establish romantic relationships with victims to manipulate the victim into sending money for fabricated emergencies or travel expenses.
- **Online Shopping and Auction Frauds**: Fraudsters create fake online stores or auction listings for non-existent or misrepresented products. Victims pay money for goods that are never delivered or are of lower value than advertised.
- **Charity Fraud:** In this fraud, the individuals' goodwill is exploited

by fraudsters by taking donations for fake charities but the money goes directly to the scammers rather than to those in need.

4.3.4 Internet Banking Fraud

Internet banking has become an integral part of modern financial transactions, providing a convenient way to pay bills, purchase goods, and transfer funds.Its ease of use and time-saving features make it a preferred method for many, eliminating the need for physical visits to banks. However, the increasing reliance on internet banking has also led to a rise in online banking fraud.

In internet banking fraud or online banking fraud, the criminals use internet or online technology to dupe the victim of their money. It can involve transferring the victim's money to different bank accounts without the permission of the victim. One of the methods to safeguard against online banking fraud is to use virtual keyboards provided by banks on their online banking portals.

4.3.4 UPI Payment Gateway Fraud

UPI has become one of the most commonly used payment methods. The UPI address is a unique virtual identifier given to a user. It follows the structure in the form of username @bank's initials. The username can be the name of a person or their mobile phone number. For example, 94351xxxxx@icici signifies a user with the mobile number 94351xxxxx who has an account with ICICI Bank.

Let us look at some of the common UPI frauds:

QR Code Scanning Scams: In this scam, fraudsters create fake QR codes and trick victims into scanning them, leading to unauthorized payments.

Fake Payment Sites: This scam involves luring victims to fake websites that mimic legitimate payment portals, prompting users to enter their UPI credentials.

Remote Access Fraud: In remote access fraud victims are

convinced to download remote control applications by which fraudsters gain access to the victims' mobile devices. Once the app is installed, the fraudster can control the victim's device remotely, including accessing UPI apps and authorizing transactions without the victim's knowledge.

4.3.5 ATM Cloning

In ATM cloning, the criminals try to clone the ATM card of the victim. To clone the ATM card, different types of machines are attached to the ATMs to scan the magnetic stripe of the ATM card. False keypads are also used over the actual keypad of the ATMs to get the PIN of the victim's ATM card. To do all this, the criminals use machines for scanning and copying the magnetic stripe of the ATM card and cameras for capturing the PIN of the user and a memory card to store all the information of the victims.

4.3.6 SIM Cloning

SIM cloning is another type of cybercrime wherein the SIM card of the victim is cloned to get financial benefits. In this type of fraud, the original SIM card is copies to get a duplicate SIM card. This can be done by using social engineering attacks like phishing etc. Once the SIM card is successfully cloned, then the criminal can access to the victim's personal details and bank account details to reset the password and PIN to obtain money from the victim.

4.4 SOCIAL ENGINEERING ATTACKS

Social engineering attacks involve malicious actions that involve human interactions and emotion related manipulations. The victim is usually tricked into making mistakes or into revealing sensitive data. In many cases, the victim is tricked into revealing confidential data or tricked into clicking malicious links or opening malicious files by evoking emotions like sense of urgency, fear etc. Social engineering attacks are difficult to prevent since

they involve a human element.

Some of the common social engineering attacks are as follows:

- Phishing
- Baiting
- Water Holing
- Pretexting
- Quid Pro Quo
- Tailgating
- Impersonation

Let us look at each of these social engineering attack in detail.

4.4.1 Phishing

Phishing is one of the most common social engineering attack. Phishing can be defined as a crime that occurs where a criminal tries to get the victim to disclose their personal and financial information by using emails. The emails sent by the fraudsters look like genuine emails by legitimate sources like banks and organizations. The victims are lured into clicking the links or downloading file from the email.

Voice phishing, commonly referred to as **vishing**, involves criminals attempting to extract personal and sensitive information from victims through voice calls.SMS phishing, or **smishing**, is a variant of phishing where fraudsters send deceptive text messages to victims' mobile phones in an attempt to trick them into divulging sensitive information or clicking on malicious links.

4.4.2 Baiting

Baiting is a cybercrime where generally physical media devices like USB are used to disperse malware to the victim's computer system. Generally, criminals leave USB devices as a bait at noticeable places with clever tags to make the employees pick and use these USB devices. When the victim uses these infected USBs, they install the malware into their computer system.

4.4.3 Water Holing

Water holingor watering hole is a cyber-attack where the attackers observe the websites that are visited by the targeted person or employees of the targeted institution. The attackers then infect those websites with malwares such that when the targeted individual visits those websites they click on malicious links or download malware into their system. The term “watering hole” is derived from the natural world, where predators often wait near watering holes to ambush their prey. Similarly, attackers wait for their targets to visit compromised websites, where they can then launch their cyber-attacks.

4.4.4 Pretexting

Pretextingis a cybercrime where the criminals based on some pretext or invented scenarios try to lure the victim in divulging secret and confidential data. In many times, criminals often start by trying to establish trust with the victim by stating that they are from right-to-know authority like police personnel and state that they need the sensitive information in order to complete a critical task.

4.4.5 Quid Pro Quo

Quid pro quo is a social engineering tactic based on the principle of reciprocity, which leverages the human tendency to feel obligated to return a favor when one is received. Quid pro quo, a Latin phrase meaning “something for something,” operates on the premise that individuals are inclined to reciprocate favors or benefits received from others. In a quid pro quo attack, the attacker exploits this natural tendency to reciprocate by offering a seemingly beneficial exchange to the victim in exchange for sensitive information or access.

4.4.6 Tailgating

Tailgating, also known as piggybacking, is a physical security

breach technique used in social engineering attacks where an unauthorized individual gains access to a secured or restricted area by closely following behind someone who has legitimate access.An example of tailgating would be a scenario where the attacker may simply walk behind the person with access to the secured area and pretend to be on a phone call, while the person who has access will open the door to the secured area out of curtesy.

4.4.7 Impersonation

Impersonation is a deceptive technique wherein an individual or entity pretends to be someone else, typically someone trusted or authoritative, in order to manipulate or deceive the target. Attackers exploit the trust placed in certain roles or positions to carry out their deceptive activities, relying on the assumption that the target will be less suspicious of communications or requests coming from familiar or authoritative sources. For example, the impersonator may impersonate a high-ranking figure within an organization, to manipulate employees into complying with fraudulent requests.



CHECK YOUR PROGRESS

Q1. What is phishing, vishing and smishing?

Q2. What is a Ponzi scheme?

4.5 MALWARE

Malware is the contraction of the term “malicious software”. Malware covers any software that intentionally tries to harm, gain access, disrupt network or interfere with the working of the user’s computer, network or server and its security aspects.It covers a wide range of harmful software types, including viruses, worms, Trojan horses, ransomware, spyware, adware, and more. Malwares are generally classified into one of the following groups listed below:

1. Virus:

The term computer virus is derived from the biological term ‘virus’for the way both viruses infect the system. Computer virus is a computer program that replicates itself and modifies other computer programs and inserts its own code into those programs when the virus code is executed. In the year 2000, the ILOVEYOU virus had impacted millions of computers. To protect against such threats, users can utilize online tools like VirusTotal website, accessible at the URL https://www.virustotal.com/gui/home/upload, where users can upload files or submit URLs to be scanned for viruses.

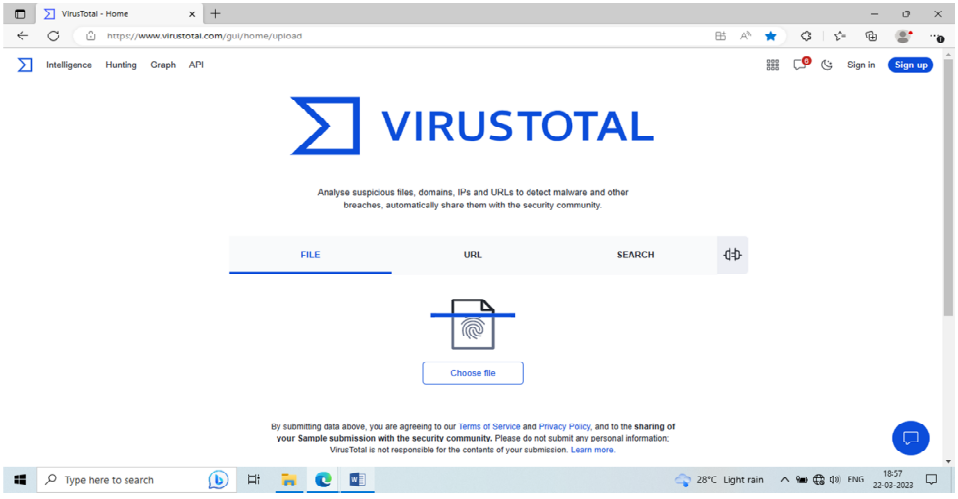


Figure 4.1: Virustotal website to check if a file or URL contains a virus

2. Worms:

A computer worm is a malwarethat spreads through computer systems using the computer network and by replicating itself. Once a worm infiltrates a system, it uses that system as a host to scan and identify other vulnerable machines within the network. The worm then attempts to infect these associated systems, continuing its spread across the network.SQL Slammer was a fast spreading worm that infected Microsoft’s SQL Server softwarein 2003 and impacted many thousands of servers.

3. Trojan Horses:

The term “Trojan Horse” originates from the ancient Greek story where Greek soldiers used a deceptive wooden horse to infiltrate and ultimately

conquer the city of Troy. In the context of cybersecurity, a Trojan Horse, or simply “Trojan,” mimics this tactic by disguising itself as a legitimate, useful software application. However, once installed, it reveals its true malicious nature, executing harmful activities without the user’s knowledge.One example of a Trojan is the Zeus Trojan, first detected in 2007 which targeted Microsoft Windows systems to steal banking credentials and financial data.

4. Ransomware:

The term “ransomware” derives from the concept of ransom in the real world, where kidnappers demand payment to release a hostage. Similarly, ransomware is a type of malicious software used by cybercriminals to extort money from victims by encrypting their data and demanding a ransom to decrypt it and restore access. This malicious act essentially holds the victim’s data hostage, with the promise of its return upon payment.One example of ransomware attacks was the WannaCry outbreak.

5. Spyware:

Spyware is a malware that collects data and information of the device and user without the knowledge of the user. The spyware is used for the purpose of spying on the activities of the user to get access to sensitive and confidential informationlike passwords or to track the internet activity of the user. DarkHotel is a spyware that uses the vulnerabilities of the hotels Wi-Fi network system to spy on specifically targetedhotel guests.

6. Keyloggers:

Keyloggers are a type of malware designed to record every keystroke made by a user on their computer. This malicious software captures detailed information, including typed emails, passwords, credit card numbers, and other sensitive data. The captured data is then sent to the attacker, often without the user’s knowledge, leading to a significant breach of privacy. Olympic Vision is a keylogger malware that was involved in Business Email Compromise (BEC) campaign that targeted many companies around the world.

7. Adware:

Adware or advertising-supported software is a malware that displays advertisements on your computer in the form of pop-ups but actually collect data of the users in the background. The adware tracks the users browsing history to collect banking data or confidential data to either use it for malicious intent or to sell it to third parties. Fireball is a browser hijacker malware which modifies settings in thebrowser of the user and blocks attempts to change or restore it back.

8. Bots and Botnets:

A botnet is a group of internet connected devices which run one or more bots. Botnets are malware used by cybercriminals to gain access to devices and computer systems to perform different types of cyberattacks and scams. Botnets can be used to either do distributed denial-of-service (DDoS) attack, record activity by using webcam or keystrokes, send phishing emails from the device or give cybercriminals remote control of the device. Mirai is a malware that turned networked devices that used Linux into remotely controlled bots and as part of a large scale botnet where most of the targeted devices were internet protocol cameras and home routers.

9. Rootkits:

Rootkit is a malware that gives control of the computer system to the cyber attacker without the user's knowledge. Rootkits are spread through phishing and malicious downloads and can be sued to install other malwares into the system. Zacinlo is a rootkit software that manipulates the operating system and anti-malware software's so that the user remains unaware of the rootkits presence in the system.

10. Fileless malware:

Fileless malware is a type of malware that uses software, applications, and protocols already built-in or native to device operating systems to install and execute malicious activities. Unlike traditional malware, it does not require downloading files, making it exceptionally difficult to detect. An example of

fileless malware is the Astaroth malware that uses fileless techniques to remain hidden on infected machines.

11. Malvertising

Malvertisingis a type of malware that uses online advertising to spread malware. It involves injecting malicious digital advertisements into legitimate online websites and webpages. Malvertising is different from adware in the sense that adware is a program that is already on the computer system and is used to track the user's web activity whereas in malvertising the attack is done online via an infected ad.

12. Wiper:

Wiper is a malware that is used to erase user or system data of the computer system it infects so that it cannot be recovered back. Cybercriminals use wipers to target computers in networks for erasing data stored in those systems and also to remove traces of an intrusion after some other malware attack. WhisperGate is an example of a wiper that is used to erase data in computer systems.

13. Scareware:

Scareware is a type of malware where the cybercriminals use social engineering to manipulate the user to buy unwanted software. In scareware attack, the users are tricked into believing that their computer system is infected with a virus and then an antivirus software is recommended that will remove the virus from their system. Most often the users have to pay for the antivirus and if the software is free then the antivirus software is non-functional or it is some kind of malware.

4.6 ZERO DAY ATTACK

Software programs when released often contain flaws or vulnerabilities in the programs that a cybercriminal can take advantage of. Software developers upon release of the software often try to find these vulnerabilities. So they analyze the code andadd patches for fixing the flaws. But when an

attacker exploits these unintentional flaws and attacks the system before the software developer or company can fix these flaws, then it is called a 'zero day' attack. The term for this attack is given as 'zero day' since there are zero number of days to fix the flaws in the software. Zero-day attack is also written a 0-day attack.

A cybercriminal can exploit vulnerabilities in various systems like operating systems, web browsers, applicationsoftware's, hardware and firmware components etc. The cybercriminals use various type of attacks to attack thevulnerable system including social engineering methods. The attacker tries to lure the user to click on malicious links using emails and messages and once the victim downloads the malware then the attacker can infiltrate the system and exploit the vulnerability. Once the vulnerability is known to the software developers, they try to fix the code by issuing patches. But, developing these patch codes take time. It can sometimes take days, weeks or months to discover the flaw and to write the code to fix those flaws. During this time, the system remains open for any cybercriminal to exploit the flaw and attack the system. Even when the patchesarereleased for the users, many do not implement these updates quickly which makes the system still vulnerable to these attacks. Zero day attacks are dangerous because only the attackers know about them and most often the cyber attackers wait for the most advantageous time to carry the attack. One of the cases of zero-day attacks was on the video conferencing application Zoom where the attackers could access the PCsof the users remotely where Windows 7 or older version of Windows were used.

Software developers look for vulnerabilities in their own software and then release patches to fix those vulnerabilities so that the systems are not exploited.One of the best ways to prevent zero-day attacks is by keeping the software's updated.

4.7 ZERO CLICK ATTACK

A zero-click attack is an attack where user intervention is not needed. The attacker can install malware or perform any other malicious attacks

without needing the user to click on any links or downloading any files that contain malware. Generally, most of the malware is downloaded into the user's mobile phones or system by tricking the users into clicking malicious links. But in case of zero click attack, the cyber criminals do not require the user to click on any link for installation of malware. This feature makes zero click attacks extremely dangerous. This means that in this kind of attacks there is less interaction and so less trace is left by criminals.

Zero-click attacks have been increasingly prevalent, particularly with the rise in smartphone use and the storage of extensive personal data. These exploits capitalize on vulnerabilities in applications that handle untrusted data, such as SMS, messaging apps, email clients, and phone applications. Since notifications display message content without user interaction, well-crafted malicious messages can exploit these vulnerabilities to install malware or perform other malicious activities on the device.



CHECK YOUR PROGRESS

Q3. What is the difference between computer virus and computer worm?

Q4. Define wiper malware.



4.8 LET US SUM UP

- **Financial fraud** occurs when individuals or organizations through deceptive, misleading and illegal practices deprives us of our money or harm our financial health.
- Identity fraud is a crime that occurs when a criminal steals or uses another person's personal information without their permission to commit a financial fraud.
- Investment fraud is a crime that occurs when criminals convinces people to invest in schemes that are have zero potential or sometimes don't even exist.

- In internet banking fraud or online banking fraud, the criminals use internet or online technology to dupe the victim of their money. It can involve transferring the victim's money to different bank accounts without the permission of the victim.
- **Social engineering attacks** involve malicious actions that involve human interactions and emotion related manipulations. The victim is usually tricked into making mistakes or into revealing sensitive data.
- Phishing can be defined as a crime that occurs where a criminal tries to get the victim to disclose their personal and financial information by using emails.
- Baiting is a cybercrime where generally physical media devices like USB are used to disperse malware to the victim's computer system.
- Pretexting is a cybercrime where the criminals based on some pretext or invented scenarios try to lure the victim in divulging secret and confidential data.
- In tailgating, the attacker will follow a person into a secured restricted area for which the attacker doesn't have any legitimate access.
- **Malware** is the contraction of the term "malicious software". Malware covers any software that intentionally tries to harm, gain access, disrupt network or interfere with the working of the user's computer, network or server and its security aspects.
- Computer virus is a computer program that replicates itself and modifies other computer programs and inserts its own code into those programs when the virus code is executed.
- A computer worm is a malware that spreads through computer systems using the computer network and by replicating itself.
- The Trojan horse is an attack where the software appears to be a legitimate useful software program to the user but once installed, the software loads its malicious functions.
- In ransomware attack, cybercriminals infect the computer system of the user to encrypt whole or part of the data and demand a ransom in order to decrypt and restore the access of the device back to the user.

- When an attacker exploits these unintentional flaws and attacks the system before the software developer or company can fix these flaws, then it is called a 'zero day' attack.
- A zero-click attack is an attack where user intervention is not needed.



4.9 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q1: Phishing can be defined as a crime that occurs where a criminal tries to get the victim to disclose their personal and financial information by using emails.Smishing or SMS phishing is a type of phishing where the criminal tries to bait the victim by using text messages from a cell phone or smartphone.Voice phishing or vishing is a crime that occurs where a criminal tries to get the victim to disclose personal and confidential information by using voice calls.

Answer to Q2: In Ponzischeme, the criminals collect money from new investors to pay existing investors. The scheme ends when no new investors join and the schemers keep the remaining money by not paying return to the old investors.

Answer to Q3: The difference between a computer virus and a computer worm is with how they replicate. Virus requires a host program and a user to execute that program whereas a worm can self-replicate and being independent.

Answer to Q4: Wiper is a malware that is used to erase user or system data of the computer system it infects so that it cannot be recovered back.



4.10 FURTHER READING

1) https://en.wikipedia.org
2) https://www.justice.gov/criminal-fraud/mass-marketing-fraud
3) https://www.kaspersky.co.in/resource-center/definitions/zero-day-exploit

4) https://www.forbes.com/sites/daveywinder/2020/07/10/zoom-confirms-zero-day-security-vulnerability-for-windows-7-users/?sh=6ca797c0753d

5) https://www.kaspersky.com/resource-center/definitions/what-is-zero-click-malware

6) https://www.checkpoint.com/cyber-hub/cyber-security/what-is-a-zero-click-attack/



4.11 MODEL QUESTIONS

Q1. Describe the different types of financial frauds.

Q2. Describe the different types of social engineering attacks.

Q3. Describe any five different types of malware.

Q4. What is a zero-day attack? How can we prevent zero-day attacks?

Q5. Explain how does zero-click attacks work.

Q6. Give the differences between adware, scareware and spyware.

Q7. What is ransomware attack? How does it take place?

Q8. Explain how does the keylogger malware work.

Q9. Explain how does the UPI payment gateway fraud happen.

Q10. Explain how does the water holing attack work.

*** ***** ***

UNIT 5 –CYBER LAW

UNIT STRUCTURE

5.1 Learning Objectives

5.2 Introduction

5.3 Cybercriminals Modus-Operandi

5.4 Reporting of Cyber Crimes

5.5 Remedial and Mitigation Measures

5.6 Legal Perspective of Cyber Crime

- 5.6.1 IT Act 2000
- 5.6.2 Amendments
- 5.6.3 Cybercrimes under IT Act

5.7 Organizations Dealing with Cybercrime and Cyber Security in India

5.8 Case Studies

5.9 Let Us Sum Up

5.10 Answers to Check Your Progress

5.11 Further Reading

5.12 Model Questions

5.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- define modus-operandi of cybercriminals
- explain how to report cyber crimes
- describe legal remedial and mitigation measures
- describe different laws that cameunder IT Act 2000 and its amendments
- list out organizations that deal with cybercrime and cyber security in India.

5.2 INTRODUCTION

In the previous unit, we have learnt about the different cybercrimes that fall under financial frauds and social engineering attacks. We have also learnt about the different types of malwares including virus, worm,

ransomware etc. Zero-day attacks and zero click attacks were also covered in detail in the previous unit.

In this unit we will learn about the modus-operandi of cyber criminals behind crimes. We will also learn about how and where to report cybercrimes in India. Remedial and mitigation measures are also discussed in this unit. The IT Act 2000 and it various amendments have also been discussed in detail in this unit. In the next unit you will be introduced to different social media platforms.

5.3 CYBERCRIMINALS MODUS-OPERANDI

Modus-operandi is a Latin term that means “mode of operating”. The term modus-operandi is mostly used when discussing crime and referencing to the methods used by criminals. Modus-operandi of cyber criminals is an identifying feature or behavioural pattern using which the criminals had committed the crime and can now be used to identify the criminal.

In the previous two units we have discussed many cybercrimes and how these crimes are committed. Depending on the cybercrime, the target and the cybercriminal the modus-operandi also varies. For example, the modus-operandi that will be employed for cybercrimes like hacking will be very different to the modus-operandi that will be applied for cyberbullying.

Some of thecommon methods used by cyber criminals are:

- Sending messages
- Making phone calls
- Sending emails
- Using social engineering attacks

5.4 REPORTING OF CYBER CRIMES

In India, cybercrimes can be reported at the website of “National Cyber Crime Reporting Portal” using the URL “https://cybercrime.gov.in/Default.aspx”. This portal is an initiative of Government of India to facilitate victims/complainants to report cybercrime complaints online. This portal caters to cybercrimes complaints only with a special focus on the

cybercrimes that are carried out against women and children.



Figure 5.1: Website of National Cyber Crime Reporting Portal

Complaint against financial frauds and a lot of other cybercrimes can be reported using the above website. Once the complaints are made, the progress made against the complaint can also be traced using the website. The tracking informationof the complaint can be received by giving the acknowledgement number and the OTP that is generated against that acknowledgement number. Depending on the crime, cybercrime complaints can also be made by lodging an FIR at the local police station. In addition to this website, cybercrimes can also be lodged using a phone call to the helpline number “1930”.

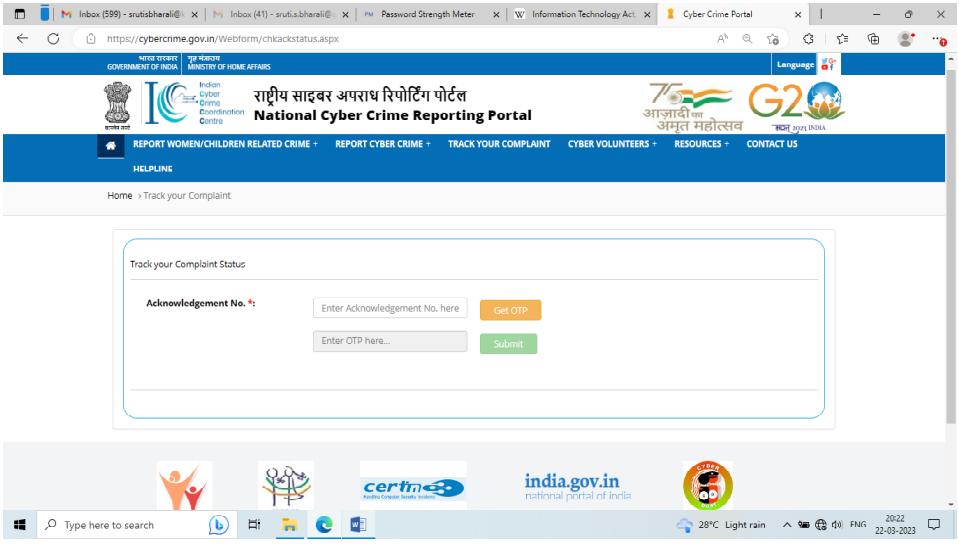


Figure 5.2: Tracking complaint status

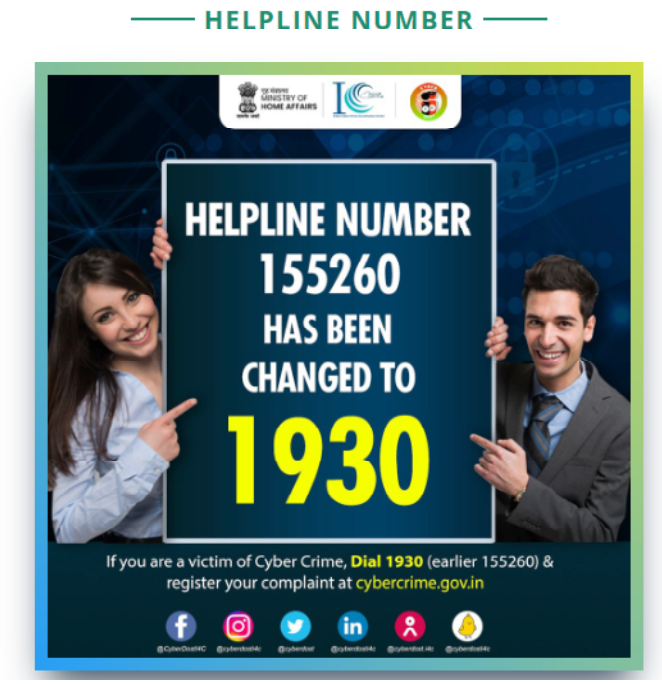


Figure 5.3: Helpline number for complaint of cybercrime

5.5 REMEDIAL AND MITIGATION MEASURES

There are various ways by which we can protect our computers and mobile devices from cybercrimes. Let us look at some of the remedial and mitigation measures that can be taken against cybercrime.

- **Update and upgrade software:** The various software that we use should be periodically updated when new versions of those software are available. The newer software versions contain not only new features but also patches of code that include protection against various virus and malware attacks.
- **Installing of anti-virus and anti-malware software's:** It is always a good idea to safeguard our electronic devices by installing and updating anti-virus and anti-malware software's. Antivirus and anti-malware software's provide an added layer of security to our devices against many cybercrimes.
- **Using strong passwords:** We should always use strong passwords for our online accounts and mainly so for internet banking, personal mail address, work mail address etc. Most of us use the same passwords for many accounts. But when

this password is not strong enough it takes cybercriminals very less time to crack it and misuse our finances and our confidential data. One of the ways to check how strong our password is to test it using the tool provided at the website Password Monster at the URL "https://www.passwordmonster.com/". For example, a password like "admin@123" can be cracked in 1.67 seconds whereas a strong password like "!I*^e$n@%$" will require 93 centuries to be cracked.

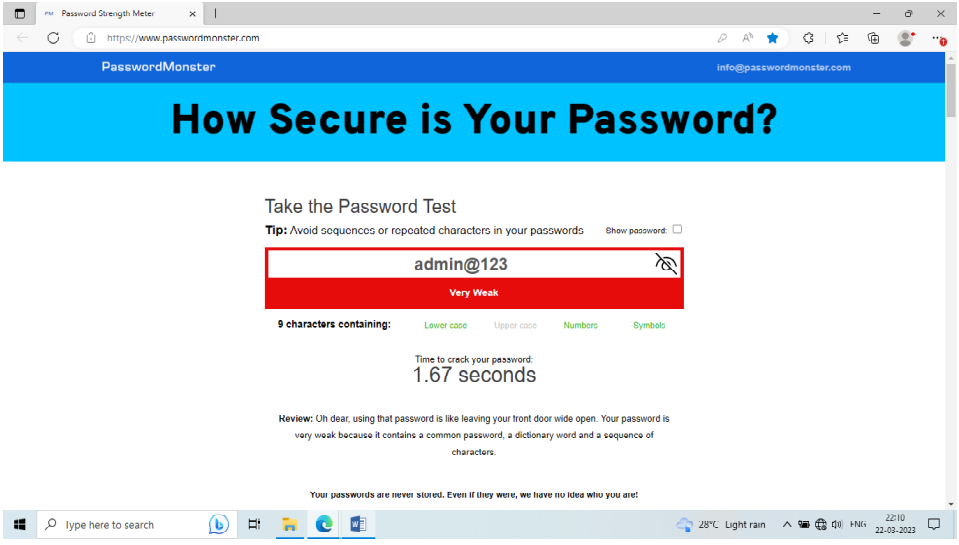


Figure 5.4: Password Test with weak password

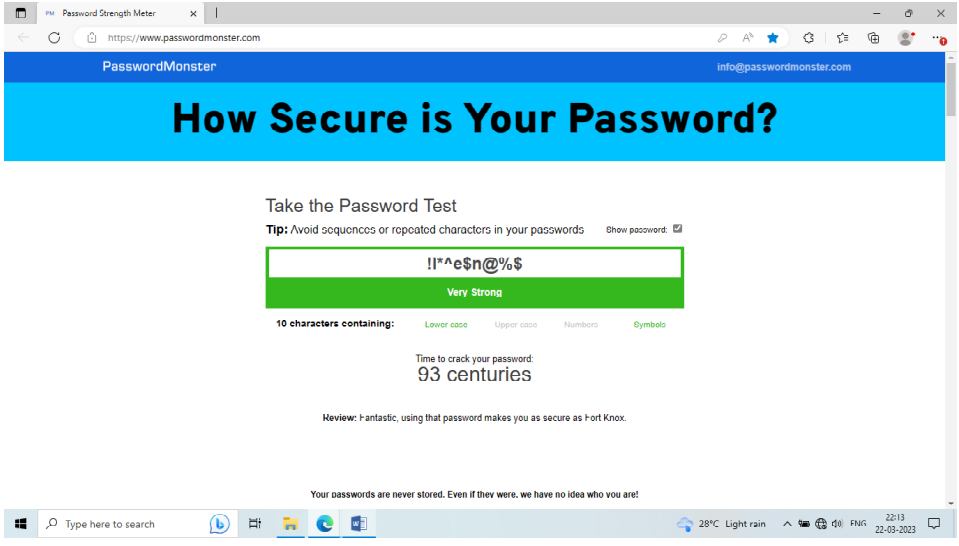


Figure 5.5: Password Test with strong password

- **Not sharing personal details:** We should be always very careful while sharing of personal or financial data. These confidential data should not be shared while casually messaging, chatting or in phone calls to random persons or to people who pose as banking officials or important government officials.

5.6 LEGAL PERSPECTIVE OF CYBER CRIME

In India, cybercrimes are covered under the Information Technology (IT) Act of 2020. The Act has been amended multiple times since the year 2020 and newer cybercrimes has been included under the law.

5.6.1 Information Technology Act 2000

The Information Technology (IT) Act, 2000 is an Act of the Indian Parliament enacted with the prime objective to create an enabling environment for commercial use of information technology. The IT Act specifies the acts which have been made punishable by law regarding cybercrime and electronic commerce in India. The IT Act has amended various sections of the Indian Penal Code (IPC) of 1860, the Indian Evidence Act of 1872, the Bankers Book of Evidence Act of 1891 and the Reverse Bank of India Act of 1934 to include cybercrimes done using new technologies.

5.6.2 Amendments

A major amendment of the IT Act was made in the year 2008. In the year 2008, section 66A was introduced which penalized for sending offensive messages. Section 69 was also introduced which gave authorities the power of “interception or monitoring or decryption of any information through any computer resource”. The amendment also included provisions for addressing issues related to pornography, child porn, cyber terrorism and voyeurism.In 2013, another amendment was made to include the offence of cyber stalking.

5.6.3 Cybercrimes under IT Act

Let us now look at the various offensesthat have been made punishable under the various sections under the IT Act.

Section	Crime
Section 65	Tampering with computer source documents.
Section 66	Computer related offences
Section 66A	Punishment for sending offensive messages through communication service, etc.
Section 66B	Punishment for dishonestly receiving stolen computer resource or communication device.
Section 66C	Punishment for identity theft.
Section 66D	Punishment for cheating by personation by using computer resource.
Section 66E	Punishment for violation of privacy.
Section 66F	Punishment for cyber terrorism.
Section 67	Punishment for publishing or transmitting obscene material in electronic form.
Section 67A	Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.
Section 67B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.
Section 67C	Preservation and retention of information by intermediaries.
Section 68	Power of Controller to give directions.
Section 69	Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
Section 69A	Power to issue directions for blocking for public access of any information through any computer resource.
Section 69B	Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.
Section 70	Protected system.
Section 71	Penalty for misrepresentation.
Section 72	Penalty for Breach of confidentiality and privacy.
Section 72A	Punishment for disclosure of information in breach of lawful contract.
Section 73	Penalty for publishing electronic signature Certificate false in certain particulars.
Section 74	Publication for fraudulent purpose.
Section 75	Act to apply for offence or contravention committed outside India.
Section 76	Confiscation.
Section 77	Compensation, penalties or confiscation not to interfere with other punishment.
Section 78	Power to investigate offences.

Some of the cybercrimes under IPC are mentioned below:

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC

- Forgery of electronic records - Sec 463 IPC
- Email spoofing - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

5.7 ORGANIZATIONS DEALING WITH CYBERCRIME AND CYBER SECURITY IN INDIA

One of the key initiatives of the Indian government to combat cybercrimes is the Indian Cyber Crime Coordination Centre (I4C). This government initiative aims to address cybercrime in India in a coordinated and effective manner and is affiliated with the Ministry of Home Affairs (MHA). It was established as a central corein the fight against cybercrime. I4C focuses on several main areas, including [7]:

- Identifying research problems and needs of law enforcement agencies and undertaking research and development activities to develop new technologies and forensic tools in collaboration with academic and research institutes in India and abroad.
- Preventing the misuse of cyberspace by extremist and terrorist groups.
- Suggesting necessary amendments to cyber laws to keep pace with rapidly changing technologies and enhancing international cooperation.
- Coordinating activities related to the implementation of Mutual Legal Assistance Treaties (MLAT) with other countries concerning cybercrimes, in consultation with the relevant nodal authority in MHA.

TheIndian Cyber Crime Coordination Centre has seven important component organizations for dealing with various issues of cybercrimes. These components are listed below [7, 8]:

1. National Cyber Crime Threat Analytics Unit (TAU): This unit generates threat intelligence reports and facilitates periodic interactions on specific cybercrimes, fostering a multi-stakeholder environment that brings together law enforcement specialists and industry experts.

2. National Cyber Crime Reporting Portal: This portal enables the reporting of all types of cybercrime incidents, with a special focus on crimes against women and children. It also automatically routes reports to the relevant State/UT.

3. National Cyber Crime Training Centre: This centre coordinates intelligence-led actions against major cybercrime threats and targets. It supports the joint identification, prioritization, preparation, and initiation of multi-jurisdictional actions against cybercrimes.

4. Cyber Crime Ecosystem Management Unit: This organization helps in forensic analysis and investigation of cybercrime using new digital technologies.

5. National Cyber Crime Research and Innovation Centre: This centre standardizes course curricula on cybercrimes, focusing on impact containment and investigations. It provides practical training on cybercrime detection, containment, and reporting in simulated environments.

6. National Cyber Crime Forensic Laboratory (NCFL) Ecosystem: This ecosystem unites academia, industry, and government to raise cybercrime awareness, establish standard operating procedures, and respond to cybercrimes.

7. Platform for Joint Cyber Crime Investigation Team: This organization tracks emerging technological developments, predicts potential vulnerabilities, and creates strategic partnerships for research and innovation in cybercrime, impact containment, and investigations.

5.8 CASE STUDIES

Let us look at some of the important case studies of cybercrimes in India.

- **Yahoo vs Akash Arora Case:**In this case, the defendant Akash Arora was accused of using the trademark or domain name 'yahooindia.com'.

This case occurred in 1999 and was one of the very first cases of cybercrime in India.

- **Job Fraud Case [9]:** The victim received an email claiming to be from Maruti Suzuki, stating that their resume had been shortlisted from Monster.com for an engineering position with a salary of Rs. 2.0 lakhs per month. The email instructed the victim to deposit Rs. 8,200 into an account and bring the pay slip to the interview, mentioning the amount was refundable. Investigations revealed the emails were sent from foreign countries, the bank account was fake, and the money was quickly withdrawn from ATMs; the criminals also contacted the victim via SMS and phone calls and were eventually arrested through mobile call tracing.
- **Baazee.com Case [10, 12]:** In December 2004, the CEO of Baazee.com was arrested because a CD with objectionable material was being sold on the website, as well as in Delhi markets. After his arrest, the Mumbai and Delhi police took action, and the CEO was later released on bail. This incident raised questions about distinguishing between Internet Service Providers and Content Providers and highlighted the need for better education on handling cybercrime cases.
- **National Association of Software and Service Companies vs. Ajay Sood& Others Case [11, 12]:** In March 2005, the Delhi High Court declared phishing to be illegal in the case of National Association of Software and Service Companies vs. Ajay Sood& Others. Phishing was described as an internet fraud where a person pretends to be a legitimate organization to extract personal data like access codes and passwords. Despite the lack of specific legislation in India against phishing, the court defined it as a misrepresentation in trade causing harm to consumers and the misused entity, treating it as passing off and tarnishing the plaintiff's image. The case, involving a placement agency falsely representing itself as Nasscom to obtain personal data, concluded with the defendants admitting their actions, highlighting the Indian judicial system's commitment to protecting IP rights.



CHECK YOUR PROGRESS

Q1. How can we report cybercrimes in India?

Q2. What are two of the amendments to the IT Act of 2000?

Q3. What are the components of I4C scheme?

Q4. What is the section that covers cyberterrorism?

ACTIVITY

1. Check how strong your password is using the **PasswordMonster**website. If your password is not strong enough, then change your password and use a good strong password in its place.



5.9 LET US SUM UP

- Modus-operandi is a Latin term that means “mode of operating”.
- Modus-operandi of cyber criminals is an identifying feature or behavioural pattern using which the criminals had committed the crime and can now be used to identify the criminal.
- In India, cybercrimes can be reported at the website of “National Cyber Crime Reporting Portal” using the URL “https://cybercrime.gov.in/Default.aspx”.
- Cybercrime complaints can also be lodged using a phone call to the helpline number “1930”.
- The Information Technology (IT) Act, 2000 is an Act of the Indian Parliament enacted with the prime objective to create an enabling environment for commercial use of information technology.
- The IT Act specifies the acts which have been made punishable by law regarding cybercrime and electronic commerce in India.
- A major amendment of the IT Act was made in the year 2008. In the

year 2008, section 66A was introduced which penalized for sending offensive messages.

- Section 69 was also introduced which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".
- The Indian Cyber Crime Coordination Centre (I4C) is a government initiative to deal with cybercrime in India in a coordinated and effective manner.
- The Indian Cyber Crime Coordination Centre has seven important component organizations for dealing with various issues of cybercrimes.



5.10 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q1: In India, cybercrimes can be reported at the website of "National Cyber Crime Reporting Portal" using the URL "https://cybercrime.gov.in/Default.aspx".

Answer to Q2: One of the amendmentwas introduced in 2008 in Section 66A which penalized for sending offensive messages. Another amendment was introduced in Section 69 was also introduced which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".

Answer to Q3: The Indian Cyber Crime Coordination Centre has seven important component organizations which are: National Cyber Crime Threat Analytics Unit (TAU), National Cyber Crime Reporting Portal, National Cyber Crime Training Centre, Cyber Crime Ecosystem Management Unit, National Cyber Crime Research and Innovation Centre, National Cyber Crime Forensic Laboratory (NCFL) Ecosystem, and Platform for Joint Cyber Crime Investigation Team.

Answer to Q4: The section that covers cyberterrorism is Section 66F.



5.11 FURTHER READING

1) https://www.soolegal.com/rc/what-are-remedies-available-for-cyber-crimes-and-cyber-defamation-under-law-
2) https://cybercrime.gov.in/Default.aspx
3) https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf
4) https://www.indiacode.nic.in/handle/123456789/1999
5) https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html
6) https://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html
7) https://i4c.mha.gov.in/
8) https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme
9) https://gurgaon.haryanapolice.gov.in/job-froud
10) https://www.indiancybersecurity.com/case_stuty_bazee.com_case.php
11) https://www.indiancybersecurity.com/case_study_nasscom_ajay_sood.php
12) https://www.cyberralegalservices.com/detail-casestudies.php



5.12 MODEL QUESTIONS

Q1. What is modus-operandi?

Q2. What are the different ways using which we can report cybercrimes in India?

Q3. Describe the objectives of I4C.

Q4. Give any two case studies of cybercrimes in India.

Q5. Describe the various legal provisions under the IT Act 2000.

Q6. Explain some of the remedial and mitigation measures that can be used against cybercrime.

Q7. What are some of the cybercrimes that came under IPC of Indian law?

Q8. Describe the IT Act 2000. Describe in brief the amendments that were made to this Act.

Q9. What is the purpose of National Cyber Crime Research and Innovation Centre?

Q10. Explain the different components of the Indian Cyber Crime Coordination Centre.

*** ***** ***

UNIT - 6: INTRODUCTION TO SOCIAL MEDIA

UNIT STRUCTURE

6.1 Learning Objectives

6.2 Introduction

6.3 Types of social media

6.4 Social media platforms

6.5 Let Us Sum Up

6.6 Further Readings

6.7 Answers to Check Your Progress

6.8 Model Questions

6.1 LEARNING OBJECTIVES

After going through this unit, you will be able to :

- explore different social media networking sites
- understand different types of social networking styes
- explain different social networking platforms

6.2 INTRODUCTION

Social media refers to a collection of digital platforms and tools that allow users to share information, create and exchange content, and connect with other peoples on that social network site. Some of the most popular social media platforms include Facebook, Twitter, Instagram, TikTok, LinkedIn, and Snapchat.

Social media has transformed the oral communications, sharing of information and connect with others peoples around the world to a new height. Social Media allows the users to create and share their own content, such as photos, videos, and written posts. It also allows the users to engage with others shared media through likes, dislikes and shares. It also allows the users to share their views on the post through comments.

Social media can be used for a wide range of purposes, from socializing and staying in touch with friends and family to promoting

businesses, brands, and products. It can also be used for political activism, social justice movements, and to raise awareness about various issues.

However, social media can also have negative effects on mental health, as it can lead to feelings of loneliness, anxiety, and depression. Additionally, social media can sometimes be a source of misinformation, cyberbullying, and online harassment. It is important for users to practice safe and responsible online behavior and to use social media in a way that promotes positive mental health and well-being.

Following are the few properties of a good social networking sites

1. User profiles: SNS allow users to create a profile that includes information about themselves, such as their name, age, location, interests, and profile picture.
2. Connections: Users can connect with other users by sending friend requests or following each other. Once a connection is made, users can see updates from their friends or connections in their news feed.
3. News feed: The news feed is a stream of content that is generated by the activity of a user's connections on the site. It can include posts, photos, videos, and other updates.
4. Communication features: SNS offer various ways for users to communicate with each other, including private messaging, commenting on posts, and group chat.
5. Content sharing: Users can share various types of content on SNS, such as photos, videos, and links to articles or websites.
6. Privacy settings: SNS typically offer users the ability to control their privacy settings, allowing them to choose who can see their profile and content.
7. Mobile accessibility: Many SNS have mobile applications, allowing users to access the platform on their mobile devices

6.3 TYPES OF SOCIAL MEDIA

There are a wide variety of social media networks available, each with its own unique features, audience, and purpose. Here we discuss some of the most popular social media networks:

Facebook: Facebook is an online social media and social networking service owned by American company Meta Platforms. It is founded by Mark Zuckerberg in 2004. This is the largest social media network with over 2.8 billion monthly active users. It allows users to connect with friends and family, join groups and communities, and share photos and videos. Facebook can be accessed from any devices with Internet connectivity, such as personal computers, tablets and smartphones. For a new user to use Facebook first need to register on Facebook by providing basic details of own. After registering, users can create profile which keeps the basic details of themselves. In Facebook users can post photos, videos and text which are basically seen by the other users on Facebook depending on different privacy settings. Users can also communicate directly with each other on Facebook via Messenger. Also, users can join common-interest groups to share views, news etc among them. It also allows the users to receive notifications on their activities at Facebook and the pages they follow.

Facebook has often been criticized over compromised with user privacy, political manipulation and mass surveillance etc. Facebook has also been subject to criticism over psychological effects such as addiction and low self-esteem, and various controversies over content such as fake news, conspiracy theories, copyright infringement, and hate speech etc.

Instagram: This platform focuses on visual content, such as photos and videos, and has over 1 billion monthly active users. It also owned by American company Meta Platforms. It is popular among influencers, brands, and businesses. It basically allows users to share photos and videos, as well as interact with other users through likes, comments and more. Instagram was launched in 2010 and has since grown to become one of the most popular social media platforms in the world. Users can create a personal profile, post content to their feed, and follow other users to see their content in their own feed. Instagram also offers features such as Stories, Reels, etc, which allow users to share short-form videos and other types of content. Instagram is available as a mobile app for iOS and Android devices, as well as a desktop website.

Twitter: This is a microblogging platform that allows users to share

short messages, known as tweets, with their followers. It has over 330 million monthly active users and is often used for news and current events, It is owned and operated by American company Twitter, Inc. Tweets can contain text, photos, videos, and links to other websites. In most cases, the text content of a Tweet can contain up to 280 characters.Twitter was launched in 2006 and has since become a popular platform for news, politics, and entertainment. Users can create a personal profile, follow other users to see their tweets in their own feed, and interact with other users by liking, retweeting, and replying to their tweets. Twitter also offers features such as hashtags, which allow users to categorize their tweets and make them more discoverable to other users. Twitter is available as a mobile app for iOS and Android devices, as well as a desktop website.

LinkedIn: This is a professional networking platform with over 740 million users. It is designed for job seekers, employers, and professionals to connect, share work-related content, and find career opportunities. It is launched in 2003 works through websites and mobile apps owned by Microsoft. LinkedIn allows users to create a professional profile that includes their work experience, education, skills, and other relevant information. Users can connect with other professionals in their field and join groups to share information and ideas. Companies can also create pages on LinkedIn to showcase their products and services and connect with potential employees. LinkedIn offers job postings and job search tools, making it a valuable resource for job seekers. Users can also share articles and other content related to their industry or profession.

TikTok: TikTok, and its Chinese counterpart Douyin is a short video hosting site owned by Chinese company ByteDance. Here users are allowed to create and share short-form videos set to music. It has over 1 billion monthly active users and is popular among younger audiences. Douyin was released in the China in September 2016. The TikTok app was launched in the international market in September 2017. In January 2019, TikTok allowed businesses to add sale links into the videos. In October 2022, TikTok was expanded into the e-commerce market in the US.

TikTok, along with 58 other Chinese-created apps, was banned

completely in India by the Ministry of Electronics and Information Technology over national security issues on 29 June 2020.

YouTube: This is a video-sharing platform with over 2 billion monthly active users. It's headquarter is in San Bruno, California. It was launched on February 14, 2005, by Steve Chen, Chad Hurley, and Jawed Karim. It is owned by Google and is the second most visited website, after Google Search. It is used for entertainment, education, and information-sharing. YouTube also offers a range of features for creators, including monetization options, live streaming, and community building tools. In addition to user-generated content, YouTube also features content from media companies, news organizations, and individual creators who produce content specifically for the platform. This content can be accessed for free, although YouTube also offers a premium subscription service called YouTube Premium, which allows users to watch videos without ads and access exclusive content. YouTube also allow advertisement and from YouTube itself it put advertisement.

Snapchat: Snapchat is a social media platform that was launched in 2011 by Evan Spiegel, Bobby Murphy, and Reggie Brown. The platform allows users to send and receive photos and videos that disappear after a set period of time, ranging from a few seconds to 24 hours. The app also includes various filters, lenses, and other features that allow users to personalize their snaps. It has over 300 million monthly active users and is popular among younger audiences.

Snapchat has become popular among younger generations due to its focus on ephemeral content and its emphasis on communication with close friends. In addition to sending snaps, users can also post Stories, which are collections of snaps that last for 24 hours and can be viewed by all of their friends.

Snapchat has also expanded its offerings to include features like Snap Map, which allows users to see the location of their friends on a map, and Discover, which features curated content from media companies, celebrities, and other sources. The platform has also introduced advertising options, allowing brands to reach Snapchat's large user base.

Pinterest: Pinterest is a social media platform that allows users to discover, save, and share ideas and inspiration through images and videos, known as pins. Users can create virtual boards to organize their pins based on themes or topics, such as recipes, home decor, travel, and fashion. The site was created by Ben Silbermann, Paul Sciarra, and Evan Sharp and its prototype was lanced in March 2011. It is operated by Pinterest, Inc.

Pinterest has over 400 million monthly active users and is available in over 30 languages. It is used by individuals for personal interests and hobbies, as well as by businesses and marketers to promote their products and services. Pinterest's algorithm uses machine learning to provide personalized recommendations to users based on their activity, interests, and behavior on the platform. Users can also search for pins and boards using keywords or browse through categories and topics.

Pinterest has been praised for its visual and user-friendly design, as well as its ability to serve as a platform for discovering new ideas and trends. However, it has also faced criticism over issues such as the spread of misinformation and the potential for promoting unrealistic or harmful beauty standards.

Other social media networks include Reddit, Tumblr, and many more. Each platform has its own unique audience and purpose, and it is important to choose the right platform for our needs and goals.

6.4 SOCIAL MEDIA PLATFORMS

There are several types of social media, each with its own unique characteristics and features. Here are some of the most common types of social media:

Social networking sites: Social networking sites are online platforms that allow users to connect and interact with others who share similar interests, backgrounds, or activities. These sites typically enable users to create a profile, share information and media, communicate with other users through messaging, comments, or chat, and join or create groups or communities. Some popular social networking sites include Facebook, Twitter, LinkedIn, Instagram, Snapchat, and TikTok. Each platform has its

unique features and target audience. For example, Facebook is used by a broad range of people for both personal and professional networking, while TikTok is primarily used by younger generations for short-form video content. Social networking sites have revolutionized the way people interact with one another and how they access and share information. However, social networking sites have also been criticized for issues such as privacy concerns, cyberbullying, addiction, and the spread of fake news and misinformation.

Microblogging platforms: Microblogging platforms are online platforms that allow users to publish short-form content, typically consisting of text, images, or video, in real-time. The content posted on microblogging platforms is usually brief and concise, often limited to a specific character or word count, such as Twitter's limit is 280-character. Some other microblogging sites are Tumblr, and Instagram. Microblogging platforms provides a popular way to users to share information and ideas with their followers and connect with others who share similar interests. They have also been used to promote products and services, as well as to drive engagement and increase brand awareness. However, microblogging platforms have also been criticized for issues such as harassment, the spread of fake news and misinformation, and censorship.

Photo sharing platforms: Photo sharing platforms are online platforms that allow users to upload, share and view photographs and images with other users. These platforms can be used for personal, social or commercial purposes, and typically provide features such as editing tools, filters, and tagging options to help users enhance and organize their photos. Some popular photo sharing platforms include Instagram, Flickr, and Google Photos. Photo sharing platforms have revolutionized the way people capture and share images, allowing anyone to take and share high-quality photos with a global audience. They have also been used by businesses and marketers to showcase their products and services and engage with their customers.

Video sharing platforms: Video sharing platforms are online platforms that allow users to upload, view, and share videos with others. These

platforms can be used for personal, social or commercial purposes and provide tools for editing and enhancing videos. Popular video sharing platforms include YouTube, Vimeo, and TikTok. Each platform has its unique features and target audience. Video sharing platforms have revolutionized the way people consume and create video content, providing anyone with the ability to produce and share their videos with a global audience. They have also been used by businesses and marketers to promote their products and services and engage with their customers.

Live streaming platforms: Live streaming is comparatively new; it is a basically provide an online platform that allow users to broadcast live video content to an audience in real-time. These platforms can be used for a variety of purposes, including entertainment, education, news, sports, and business. Some popular live streaming platforms are Twitch, YouTube Live, Facebook Live, and Instagram Live. Each platform has its unique features and target audience. For example, Twitch is a popular platform for live streaming video games and e-sports, while Facebook Live is often used for personal and community events. Live streaming platforms help users to engage with their audience in real-time. They have also been used by businesses and marketers to promote their products and services and connect with their customers in new and innovative ways.

Discussion forums: Discussion forums are online platforms that is used for conversation on some topic. Here users participate in discussions with other users on a variety of topics. These platforms can be used for personal, social, educational or professional purposes, and provide a space for users to ask questions, share ideas, and connect with others who share similar interests. Some popular discussion forum platforms include Reddit, Quora, and Stack Overflow. Discussion forums are popular among the users to learn, connect, and collaborate with others. For example, Stack Overflow is used by the programmer to share their program codes and discuss about different errors occurred in programming.

Social bookmarking sites: Social bookmarking sites are online platforms that allow users to save and organize bookmarks or web pages and share them with other users. These platforms can be used for personal

or professional purposes, and provide a way for users to discover and curate content from around the web. Some popular social bookmarking sites include Pinterest, Pocket, and Reddit. However, social bookmarking sites have also faced criticism for issues such as the spread of misinformation and spam, and the potential for promoting toxic or harmful content.

Virtual reality platforms: Virtual reality platforms are online platforms that allow users to experience immersive, computer-generated environments through the use of virtual reality headsets and other devices. These platforms can be used for a variety of purposes, including entertainment, education, training, and therapy. Some popular virtual reality platforms include Oculus, HTC Vive, and PlayStation VR. Each platform has its unique features and target audience. Virtual reality platforms have faced criticism for issues such as the potential for promoting addictive behavior, the risk of motion sickness, and the potential for disconnecting users from the real world.

Blogging platforms: These platforms allow users to create and publish their own written content, such as articles and essays. Examples include WordPress and Medium. These platforms can be used for personal or professional purposes, and provide a way for users to share their ideas, opinions, and experiences with a global audience. Blogging platforms have become an important tool for content creation and distribution, providing a space for people to share their stories and ideas with others. They have also been used by businesses and marketers to promote their products and services and connect with their customers in a more personal and engaging way.

These are just a few examples of the many types of social media available today. Each type of social media serves a different purpose and offers unique opportunities for communication, connection, and engagement.



CHECK YOUR PROGRESS

1. What does the acronym “SNS” stand for?
   a) Social Network System
   b) Social Networking Site
   c) Social Network Software
   d) Social Network Sharing
2. Which of the following is NOT a social media networking site?
   a) Facebook b) LinkedIn
   c) Instagram d) WhatsApp
3. What is a hashtag?
   a) A type of social media platform
   b) A way to tag and categorize content on social media
   c) A type of private messaging feature
   d) A way to connect with other users on social media
4. What is the character limit for a tweet on Twitter?
   a) 140 b) 280
   c) 500 d) 1000
5. Which social media platform mainly build to share short videos?
   a) Facebook b) Twitter
   c) TikTok d) LinkedIn



6.5 LET US SUM UP

- Social media refers to a collection of online platforms and tools that enable individuals and groups to create, share, and exchange information, ideas, and content with each other. These platforms include popular websites such as Facebook, Twitter, Instagram, LinkedIn, and YouTube, among others.

- Social media has become a significant aspect of modern society, affecting communication, culture, politics, and commerce. It allows individuals and groups to connect and communicate with each other, share and consume news and information, build and maintain relationships, and engage in social and political activism.
- Social media platforms typically offer users a range of features, including user profiles, connections with other users, news feeds, communication tools, content sharing, privacy settings, and algorithmic curation.
- Social media also presents numerous opportunities and challenges for individuals, organizations, and society as a whole, including issues related to privacy, data security, cyberbullying, fake news, and disinformation.
- There are different social media platforms like video sharing sites, photo sharing sites chatting sites etc.



6.6 FURTHER READINGS

1) “The Social Media Bible: Tactics, Tools, and Strategies for Business Success” by Lon Safko and David K. Brake
2) “Social Media Marketing All-in-One For Dummies” by Jan Zimmerman and Deborah Ng
3) “Socialnomics: How Social Media Transforms the Way We Live and Do Business” by Erik Qualman
4) “The Art of Social Media: Power Tips for Power Users” by Guy Kawasaki and Peg Fitzpatrick
5) “Likeable Social Media: How to Delight Your Customers, Create an Irresistible Brand, and Be Amazing on Facebook, Twitter, LinkedIn, Instagram, Pinterest, and More” by Dave Kerpen



6.7 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q. No. 1: b) Social Networking Site

Ans to Q. No. 2: d) WhatsApp

Ans to Q. No. 3: b) A way to tag and categorize content on social media

Ans to Q. No. 4: b) 280

Ans to Q. No. 5: c) TikTok



6.8 MODEL QUESTIONS

Q1. What is social media, and how does it work?

Q2. What are the benefits and drawbacks of using social media?

Q3. How has social media changed the way people communicate and connect with each other?

Q4. How do businesses use social media for marketing and engagement?

Q5. Write a short note on different social media platforms.

Q6. Write short notes on Facebook and Instagram.

*** ***** ***

UNIT - 7: HANDLING SOCIAL MEDIA

UNIT STRUCTURE

7.1 Learning Objectives

7.2 Introduction

7.3 Social media Monitoring

7.4 Hashtag in Social Media

7.5 Viral Content

7.6 Social Media Marketing

7.7 Privacy in Social Media

7.8 Challenges, Opportunities and Pitfalls in Social Media

7.9 Let Us Sum Up

7.10 Further Readings

7.11 Answers to Check Your Progress

7.12 Model Questions

7.1 LEARNING OBJECTIVES

After going through this unit, you will be able to know

- define social media monitoring
- define hashtag and viral content
- understand social media marketing
- explore privacy, challenges, opportunities and pitfalls in social media

7.2 INTRODUCTION

In this unit, we will learn about social marketing. We will explore what viral content is in social media and the key factors that help content go viral. We will also discuss privacy issues, challenges, opportunities, and pitfalls related to social media. Additionaly, we will understand how social media marketing works and how social media platforms collect data for marketing purposes.

7.3 SOCIAL MEDIA MONITORING

Social media monitoring refers to tracking and analyzing contents, conversations, feedback etc. across various social media platforms. The goal of social media monitoring is to gather insights and details from the users. For example, if it is a business product then it comes to gather reviews from customers, whereas for a political party it is about to collecting interest and need from the voters, for a musician it is about the likes/ dislikes of audiences. These types of information help in decision-making for respective counterpart.

Here are some of the key benefits of social media monitoring:

Brand reputation management: By monitoring of social media businesses can track and manage their online reputation by looking at comments, reviews and feedbacks of their brand or products by the consumers and can make strategies for the same so that brand gain more consumer attention.

Customer insights: By observing social media businesses can know about the customers interest area, likes and dislike of the customer. By gathering this type of information business can do needful for including customer preferences, understanding pain points and add more opinions.

Competitive analysis: By analysis the social media data one businesses can know about what other businesses are doing and can compare with other businesses, also can monitor competitors' social media activity, including their marketing strategies and customer engagement.

Crisis management: Social media monitoring enables businesses to quickly identify and respond to potential crisis situations, such as negative customer feedback and complaints and it allow businesses to take quick action to mitigate it.

Social media engagement: Social media monitoring helps businesses stay engaged with their customers by responding to their questions, comments, and feedback and it helps in a great way for direct communication with the customers.

There are several tools and software available for social media monitoring, such as Hootsuite, Sprout Social, and Brandwatch. These tools allow businesses to track and analyze social media activity across multiple platforms, set up alerts and notifications, and generate reports and insights.

Following is brief description of some popular social media monitoring tools:

Hootsuite - A popular social media management tool that offers a suite of features, including social media monitoring, scheduling, and reporting.

Sprout Social - A social media management and optimization platform that includes social media monitoring, analytics, publishing, and engagement tools.

Mention - A real-time media monitoring and analytics tool that allows users to track mentions of their brand or competitors across various channels, including social media, news sites, and blogs.

Brand24 - A social media listening tool that tracks mentions of a brand or specific keywords on various platforms and provides insights on sentiment, reach, and engagement.

Awario - A social media monitoring tool that tracks mentions of a brand or keywords across various channels, including social media, blogs, and news sites, and provides insights on sentiment and reach.

Agora Pulse - A social media management tool that includes social media monitoring, scheduling, publishing, and analytics features.

Zoho Social - A social media management tool that offers social media monitoring, publishing, collaboration, and analytics features.

Talkwalker - A social media monitoring and analytics tool that tracks mentions of a brand or keywords across various channels and provides insights on sentiment, reach, and engagement.

Meltwater - A media intelligence and social media monitoring tool that tracks mentions of a brand or keywords across various channels and provides insights on sentiment, reach, and engagement.

Brandwatch - A social listening and analytics tool that tracks mentions of a brand or keywords across various channels, including social media, news sites, and forums, and provides insights on sentiment, reach, and engagement.

7.4 HASHTAG IN SOCIAL MEDIA

A hashtag is a word or phrase preceded by the hash (#) symbol that is used on social media platforms to categorize content and make it easier to find and track. Hashtags are a powerful tool for social media marketing and engagement, and they are commonly used on platforms like Twitter, Instagram, and TikTok.

Here are some key ways in which hashtags are used on social media:

Categorization: Hashtags are used to categorize content according to topic, theme, and event. For example, a post about a new restaurant opening might include the hashtags #foodie or #newrestaurant.

Discovery: Hashtags are used to make content more discoverable by users who are interested in a particular topic. Users can search for hashtags to find content related to that topic or follow hashtags to see new content in their feed.

Branding: Hashtags are often used as a branding tool to promote a business, product, or campaign. For example, a clothing brand might use the hashtag #FashionForward to promote its latest collection.

Community building: Hashtags are used to build communities around shared interests or causes. For example, the hashtag #BlackLivesMatter has been used to build a community around the social justice movement.

Campaign tracking: Hashtags are used to promote social movement or agitation against the govt etc. also used to track the success of the campaigns and measure engagement. For example, a social media campaign might include a unique hashtag to track how many users are sharing and engaging with the campaign.

When using hashtags, it's important to choose relevant and specific keywords that accurately describe the content being shared. Using too many hashtags or irrelevant hashtags can make posts look spammy and reduce engagement.

7.5 VIRAL CONTENT

Viral content is the content that spreads rapidly and widely across social media platforms through likes, shares, and comments. Viral content can be anything from a funny meme or video to a breaking news story or a heart-warming moment. The key characteristic of viral content is that it resonates with a large number of people and inspires them to share it with others.

Following are few requirements for vital content on social media content:

Emotional appeal: Content that evokes strong emotions, such as happiness, anger, or awe, is more likely to go viral. People are more likely to share content that elicits an emotional response from them.

Novelty: Content that is unique, unexpected, unexplored or surprising is more likely to grab people's attention and encourage them to share it with others.

Relevance: Content that is relevant to current events, trends, or cultural moments is more likely to go viral. People are more likely to share content that is timely and relevant to their interests.

Shareability: Content that is easy to share and distribute across social media platforms is more likely to go viral. Content that is visually appealing, has a clear message, and is easy to understand is more likely to be shared.

Influencers: Content that is shared by social media influencers or celebrities is more likely to go viral. Influencers have large followings and can amplify the reach of viral content.

Creating viral content is not an exact science, but understanding what factors contribute to the virality of social media content can help businesses and individuals create content that is more likely to be shared and seen by a wider audience.

7.6 SOCIAL MEDIA MARKETING

Social media marketing is about to use social media platforms to promote a brand, product, or service among the users of social media and potential customers. Social media marketing involves creating and sharing content on social media platforms, as well as using paid advertising and analytics to measure and optimize marketing efforts.

Key components of social media marketing:

Content creation: Social media marketing involves creating and sharing content, such as images, videos, and blog posts on social media platforms. Content should be engaging, informative, and relevant to the target audience.

Audience engagement: Social media marketing involves engaging with customers and potential customers through comments, messages, and other forms of communication. This helps build relationships and foster brand loyalty.

Paid advertising: Social media marketing can also involve paid advertising, such as promoted posts or sponsored ads, to reach a wider audience and target specific demographics.

Analytics and tracking: Social media marketing involves tracking and analyzing metrics, such as engagement rates and conversion rates, to measure the success of marketing efforts and make data-driven decisions.

Some popular social media platforms for marketing include Facebook, Instagram, Twitter, LinkedIn, and TikTok. Each platform has its own strengths and weaknesses, as well as unique audience demographics, so it's important for businesses to choose the platforms that align with their marketing goals and target audience.

Social media marketing can be an effective way for businesses to reach and engage with customers, build brand awareness, and drive conversions. However, it's important to have a clear strategy and understanding of the target audience and metrics to ensure that marketing efforts are effective and efficient.

7.7 PRIVACY IN SOCIAL MEDIA

Social media is used by almost everybody in one way or other. Now a days for young generation it seems life is incomplete without social media, or we can say we human beings survive on food, water, air and social media. Peoples are dependent to such an extent that everyone tend to share every bit of information on social media platform. The main revenue source for the social media is advertisements. Moreover, social media sites like Facebook, Instagram maintains a brief profile about each users likes and dislikes what the user browses on the internet and according to that they put the advertisement according to that on their social media feeds. Even some social media sites collect information what users are doing when they are offline where they like to go which shops, they used to visit what the friends of the user likes and dislikes etc.

Here are some key aspects of privacy in social media:

Data collection: Social media platforms collect data from users, including personal information, browsing behavior, and location. This data can be used for targeted advertising and other purposes, so it's important to understand and manage privacy settings to control what data is collected and how it's used.

Privacy settings: Social media platforms offer privacy settings that allow users to control who can see their posts, profile information, and activity. It's important to review and adjust these settings regularly to ensure that personal information is only visible to intended audiences.

Third-party apps: Social media platforms often integrate with third-party apps and services, which can access user data. It's important to review and understand the privacy policies of these apps and services before granting access to personal information.

Cybersecurity: Social media platforms can be vulnerable to cyber-attacks, such as hacking or phishing scams. It's important to use strong passwords and enable two-factor authentication to protect personal information from unauthorized access.

Legal issues: Social media platforms are subject to laws and regulations related to privacy and data protection. It's important to be aware of these laws and regulations and to report any privacy violations to the appropriate authorities.

Overall, it's important for social media users to be aware of the privacy implications of using these platforms and to take steps to protect their personal information. This includes understanding and managing privacy settings, being cautious about sharing sensitive information, and using strong cybersecurity practices.

For keeping each your data private you need to read the privacy policy of social media carefully. Following are some tips

1. Read the Terms and Conditions of social networking sites carefully.
2. Set the privacy settings of the account according to the need.
3. Avoid clicking third party link like "Check your Marriage Date", "Won prize" and so on.
4. Use reputed antivirus software for your devices.
5. Turn off location access. Remove access to your device data. Because some sites even keep track of user activities in the offline world too.
6. Don't forget to set the Security Answers.
7. Don't browse your account from public devices. And logout from the account when you done browsing.
8. Always analyze the post before posting. Do not share private data on social media.
9. Always set a strong password and change it in regular interval. Never set same passwords for multiple sites.

7.8 CHALLENGES, OPPORTUNITIES AND PITFALLS IN SOCIAL MEDIA

Following are the challenges of social media:

Privacy concerns: Users of online social networks may have their personal information, browsing behavior, and location tracked and used for targeted advertising, among other purposes. This can raise concerns about privacy and data security.

Cyberbullying: Online social networks can provide a platform for cyberbullying and harassment, which can have serious emotional and psychological consequences for victims.

Misinformation and fake news: Online social networks can be a breeding ground for misinformation and fake news, which can spread rapidly and have serious implications for individuals and society.

Addiction: The constant stream of information and notifications on online social networks can be addictive, leading to negative effects on mental health and wellbeing.

Following are the opportunities of social media:

Communication: Online social networks provide a convenient and accessible way for people to communicate and connect with one another across the globe.

Business opportunities: Online social networks offer businesses a way to reach and engage with customers, build brand awareness, and drive conversions.

Education: Online social networks can be used as a tool for education, providing access to educational resources and facilitating collaboration among students and teachers.

Social activism: Online social networks can be a powerful tool for social activism, allowing people to raise awareness about social and political issues and organize grassroots movements.

Following are the Pitfalls of social media:

Information overload: The constant stream of information on online social networks can be overwhelming, leading to information overload and cognitive overload.

Filter bubbles: Online social networks can create filter bubbles, where users are exposed only to information and opinions that confirm their existing beliefs, leading to polarization and division.

Addiction: The addictive nature of online social networks can lead to negative effects on mental health and wellbeing, including depression, anxiety, and low self-esteem.

Time management: The constant distraction of online social networks can make it difficult to manage time effectively and stay focused on important tasks.

Overall, online social networks offer both opportunities and challenges. It is important for individuals and society as a whole to be aware of these challenges and to take steps to address them while embracing the opportunities that online social networks present.



CHECK YOUR PROGRESS

State True or False

1. Social media monitoring involves tracking and analyzing social media platforms to gain insights about individuals, brands, or topics.
2. Social media monitoring can be used for market research and competitive analysis.
3. Social media monitoring tools can provide real-time alerts and notifications for brand mentions and keywords.
4. Social media monitoring is only useful for businesses with a large social media presence.
5. Social media monitoring is primarily used for tracking customer complaints and negative feedback.



7.9 LET US SUM UP

- Social media monitoring is the process of tracking and analyzing social media platforms to gain insights about individuals, brands, or topics.
- A hashtag is a keyword or phrase preceded by the # symbol that is used on social media platforms to categorize and organize content related to a specific topic.
- Viral content refers to online media, such as a video, image, or article, that spreads rapidly and widely through social media sharing, often achieving widespread popularity or notoriety.

- Privacy in social media refers to an individual's right to control and manage their personal information and data shared on social media platforms.
- Social media marketing is the use of social media platforms to promote a product or service and engage with customers to build a brand and increase sales.
- Opportunities in social media refer to the potential benefits and advantages that can be gained from utilizing social media platforms, such as increased brand visibility, customer engagement, and the ability to target specific audiences.
- Challenges in social media refer to the potential risks and obstacles associated with using social media, such as managing online reputation, dealing with negative feedback, and protecting user privacy.
- Pitfalls in social media refer to the potential dangers and drawbacks associated with using social media, such as cyberbullying, addiction, misinformation, and the spread of fake news.



7.10FURTHER READINGS

1) "The Social Media Bible: Tactics, Tools, and Strategies for Business Success" by Lon Safko and David K. Brake
2) "Social Media Marketing All-in-One For Dummies" by Jan Zimmerman and Deborah Ng
3) "Socialnomics: How Social Media Transforms the Way We Live and Do Business" by Erik Qualman
4) "The Art of Social Media: Power Tips for Power Users" by Guy Kawasaki and Peg Fitzpatrick
5) "Likeable Social Media: How to Delight Your Customers, Create an Irresistible Brand, and Be Amazing on Facebook, Twitter, LinkedIn, Instagram, Pinterest, and More" by Dave Kerpen

7.11 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q. No. 1: True

Ans to Q. No. 2: True

Ans to Q. No. 3: True

Ans to Q. No. 5: False

Ans to Q. No. 5: False

7.12 MODEL QUESTIONS

Q1. What are the benefits of social media monitoring for businesses?

Q2. What are the best practices for using hashtags on social media?

Q3. What are the key elements of content that can make it go viral?

Q4. What are some common privacy concerns associated with using social media?

Q5. How can individuals protect their privacy on social media platforms?

Q6. What are the biggest challenges businesses face when using social media for marketing?

Q7. What are the benefits of using social media for customer service?

*** ***** ***

UNIT 8: SECURITY ISSUES IN SOCIAL MEDIA

UNIT STRUCTURE

8.1 Learning Objective

8.2 Introduction

8.3 Issues with Social Media Security

8.4 Reporting and Flagging of Offensive Content

8.5 Laws Governing the Publication of Offensive Material

8.7 Best Practices for The Use of Social Media

8.8 Case Studies

8.9 Let Us Sum Up

8.10 Answers to Check Your Progress

8.11 Further readings

8.12 Model Questions

8.1 LEARNING OBJECTIVE

After going through this unit, you will be able to:

- identify potential security risks associated with social media usage.
- evaluate the effectiveness of privacy settings on social media platforms.
- develop strategies for protecting personal information while using social media.
- analyse the impact of social media on personal and professional reputation.
- create a plan to respond to security breaches or unauthorized access to social media accounts.

8.2 INTRODUCTION

Social media has become an inseparable part of our lives, with billions of people using various platforms to connect, share information, and express themselves. While social media has many benefits, it also poses security

risks that users must be aware of. From cyberbullying and online harassment to data breaches and identity theft, the security issues on social media can have serious consequences. It is essential for users to take proactive measures to protect their privacy and security on social media platforms.

In this unit, first, we'll discuss the issues associated with social media security. We will also discuss governmental regulations and flagging offensive content. We'll learn about using social media best practices and understand some case studies in the end.

8.3 ISSUES WITH SOCIAL MEDIA SECURITY

Social media has revolutionized the way people connect and interact with one another. However, with the increasing use of social media platforms, the issue of social media security has become a major concern. Here are some of the main issues with social media security:

1. Privacy: One of the biggest issues with social media security is privacy. Many social media platforms collect user data and information, which can be used for targeted advertising and other purposes. Users may not be aware of how their data is being collected and used, and their personal information may be vulnerable to theft or misuse.
2. Cyberbullying: Another issue with social media security is cyberbullying. Social media provides a platform for individuals to harass, intimidate, or threaten others online, often anonymously. Cyberbullying can have serious consequences for its victims, including depression, anxiety, and even suicide.
3. Identity theft: Social media platforms often require users to provide personal information, such as their name, email address, and date of birth. This information can be used by cybercriminals to steal the user's identity and commit fraud.
4. Malware: Social media platforms are also susceptible to malware attacks. Cybercriminals can use social media to spread malware through fake links and downloads, which can compromise the security of users' devices.

5. Fake accounts: Social media platforms are also vulnerable to fake accounts. These accounts can be used to spread misinformation, propaganda, and other types of harmful content.

To address these issues, social media platforms have implemented security measures such as two-factor authentication, privacy settings, and content moderation. However, users should also take steps to protect their own privacy and security, such as using strong passwords, avoiding sharing sensitive information online, and being cautious about accepting friend requests from strangers.

8.4 REPORTING AND FLAGGING OF OFFENSIVE CONTENT

Reporting and flagging offensive content is an important way for social media users to help keep online spaces safe and inclusive. Offensive content can take many forms, including hate speech, cyberbullying, harassment, and graphic or violent content. Here are some key points to consider when reporting or flagging offensive content:

1. Know the platform's policies: Social media platforms have different policies and guidelines for what content is considered offensive or inappropriate. Before reporting or flagging content, be sure to familiarize yourself with the platform's policies and guidelines.
2. Report content promptly: When you encounter offensive content, it's important to report it promptly. Reporting or flagging content can help prevent others from being exposed to harmful or offensive content.
3. Provide specific details: When reporting or flagging content, provide as much specific detail as possible, including the location of the content (e.g., URL or post ID), the type of content, and the reason for your report.
4. Avoid retaliatory behaviour: If you encounter offensive content, it's important to avoid retaliatory behaviour. Engaging with offensive content or users can escalate the situation and lead to more harm.
5. Understand the limitations: While reporting or flagging offensive content

can be an effective way to keep online spaces safe, it's important to understand that there are limitations to what can be done. Social media platforms may not always be able to take action on reported content, and the process can take time.



CHECK YOUR PROGRESS

1. What are some of the main issues with social media security?
2. What are some key points to consider when reporting or flagging offensive content on social media?

By reporting or flagging offensive content, social media users can help create a safer and more inclusive online community. However, it's important to remember that reporting and flagging is just one part of the solution. We all have a role to play in promoting respectful and positive online interactions.

8.5 LAWS GOVERNING THE PUBLICATION OF OFFENSIVE MATERIAL

The publication of offensive material on social media platforms is a complex issue, and laws governing this area can vary depending on the country or jurisdiction. Offensive material can include hate speech, defamatory content, or sexually explicit content. Here are some general points to consider when it comes to laws governing the publication of offensive material in social media:

- Understand the local laws: Different countries have different laws governing the publication of offensive material on social media platforms. It's important to understand the legal framework in your country or jurisdiction.
- Know the definitions of offensive material: Laws may have different definitions of what constitutes offensive material in social media. It's important to be aware of these definitions to avoid unintentional violations.

- Be aware of consequences: The consequences for publishing offensive material in social media can be serious, including fines, legal action, or even imprisonment.
- Consider the impact on others: The publication of offensive material in social media can have a harmful impact on others, including vulnerable or marginalized communities. Consider the potential impact of your content before publishing.
- Seek legal advice: If you are unsure about the legality of publishing certain content on social media, seek legal advice to ensure that you are in compliance with local laws.

In general, it is important to be mindful of the content you publish on social media and to ensure that it does not violate any laws or harm others. By being aware of the legal framework and seeking legal advice when necessary, you can help ensure that your online presence is responsible and respectful. Additionally, social media companies also have a responsibility to enforce their own community guidelines and policies to prevent the publication of offensive material on their platforms.

International Laws:

International laws governing the publication of offensive material in social media can be complex and vary depending on the country or jurisdiction. However, there are some international agreements and frameworks that can provide guidance in this area. Here are some key points to consider:

1. Universal Declaration of Human Rights: The Universal Declaration of Human Rights (UDHR) is a global agreement that outlines fundamental human rights. Article 19 of the UDHR protects the right to freedom of expression, but also recognizes that this right may be subject to restrictions for the protection of national security, public order, or the rights of others.
2. International Covenant on Civil and Political Rights: The International Covenant on Civil and Political Rights (ICCPR) is a treaty that protects a range of civil and political rights. Article 19 of the ICCPR protects the

right to freedom of expression, but also recognizes that this right may be subject to restrictions for the protection of national security, public order, or the rights of others.

3. International Convention on the Elimination of All Forms of Racial Discrimination: The International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) is a treaty that prohibits racial discrimination and promotes racial equality. Article 4 of the ICERD requires states to criminalize hate speech that incites discrimination, hostility, or violence.
4. European Convention on Human Rights: The European Convention on Human Rights (ECHR) is a treaty that protects a range of human rights in Europe. Article 10 of the ECHR protects the right to freedom of expression, but also recognizes that this right may be subject to restrictions for the protection of national security, public safety, or the rights of others.
5. Social media platforms' terms of service: Social media platforms often have their own terms of service that outline acceptable use policies and prohibit the publication of offensive material. Violations of these terms can result in the removal of content or even the suspension or termination of accounts.

While laws governing the publication of offensive material in social media can be complex and vary depending on the jurisdiction, it is important to be aware of these laws and to ensure that your online presence is responsible and respectful. By being mindful of the content you publish online and by respecting the rights and dignity of others, you can help create a safer and more inclusive online community.

Indian Laws:

International laws governing the publication of offensive material in social media can be complex and vary depending on the country or jurisdiction. However, there are some international agreements and frameworks that can provide guidance in this area. Here are some key points to consider:

1. Universal Declaration of Human Rights: The Universal Declaration of Human Rights (UDHR) is a global agreement that outlines fundamental human rights. Article 19 of the UDHR protects the right to freedom of expression, but also recognizes that this right may be subject to restrictions for the protection of national security, public order, or the rights of others.
2. International Covenant on Civil and Political Rights: The International Covenant on Civil and Political Rights (ICCPR) is a treaty that protects a range of civil and political rights. Article 19 of the ICCPR protects the right to freedom of expression, but also recognizes that this right may be subject to restrictions for the protection of national security, public order, or the rights of others.
3. International Convention on the Elimination of All Forms of Racial Discrimination: The International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) is a treaty that prohibits racial discrimination and promotes racial equality. Article 4 of the ICERD requires states to criminalize hate speech that incites discrimination, hostility, or violence.
4. European Convention on Human Rights: The European Convention on Human Rights (ECHR) is a treaty that protects a range of human rights in Europe. Article 10 of the ECHR protects the right to freedom of expression, but also recognizes that this right may be subject to restrictions for the protection of national security, public safety, or the rights of others.
5. Social media platforms' terms of service: Social media platforms often have their own terms of service that outline acceptable use policies and prohibit the publication of offensive material. Violations of these terms can result in the removal of content or even the suspension or termination of accounts.

While laws governing the publication of offensive material in social media can be complex and vary depending on the jurisdiction, it is important to be aware of these laws and to ensure that your online presence is responsible and respectful. By being mindful of the content you publish online

and by respecting the rights and dignity of others, you can help create a safer and more inclusive online community.



CHECK YOUR PROGRESS

3. What are some general points to consider when it comes to laws governing the publication of offensive material in social media?
4. What are some international agreements and frameworks that provide guidance in the area of laws governing the publication of offensive material in social media?

8.7 BEST PRACTICES FOR THE USE OF SOCIAL MEDIA

Social media has become an integral part of our daily lives, and it is important to use it responsibly and effectively. Here are some best practices for the use of social media:

1. Be aware of your audience: Consider who your intended audience is and adjust your content accordingly. What might be appropriate for one audience may not be appropriate for another.
2. Think before you post: Take a moment to consider the potential impact of your content before you post it. Ask yourself if it could be offensive or harmful to others, or if it could be misinterpreted in any way.
3. Be respectful: Treat others with respect and kindness on social media, even if you disagree with them. Avoid engaging in arguments or negative interactions that could escalate.
4. Protect your privacy: Be mindful of the personal information you share on social media, and adjust your privacy settings to limit who can see your posts and personal details.
5. Stay informed: Keep up to date with the latest social media trends and updates, and be aware of any changes in the platform's policies and guidelines.
6. Give credit where it's due: If you share content created by others, make

sure to give credit where it's due. This can include tagging the creator or citing the source of the content.

7. Use social media for positive purposes: Social media can be a powerful tool for sharing positive messages and promoting social change. Consider using your platform to raise awareness about important issues or to spread kindness and positivity.

By following these best practices, you can help ensure that your use of social media is responsible, effective, and respectful. It can also help to create a positive and supportive online community.

8.8 CASE STUDIES

Around the world, there are numerous instances of social media security problems. a few examples are provided below.

1. The Cambridge Analytica scandal is a well-known case that highlights the security issues related to social media platforms. Cambridge Analytica was a political consulting firm that obtained data from millions of Facebook users without their knowledge or consent. The firm used this data to create targeted political advertising during the 2016 US presidential election campaign.The scandal began when a Cambridge University professor, Aleksandr Kogan, created a personality quiz app that was used by approximately 270,000 Facebook users. However, the app also collected data from the users' Facebook friends, which ultimately resulted in the collection of data from millions of users without their consent. This data was then sold to Cambridge Analytica, which used it to create targeted political advertising for the Trump campaign.The scandal raised concerns about the security of personal data on social media platforms, as well as the use of targeted advertising in political campaigns. Facebook faced significant criticism for its role in the scandal, including accusations that it had failed to properly protect user data and had not done enough to prevent the misuse of its platform.The Cambridge Analytica scandal led to a number of changes in the way that Facebook and other social media platforms handle user

data. For example, Facebook introduced new privacy settings and restrictions on third-party apps. The scandal also highlighted the need for increased transparency and accountability in the use of personal data on social media platforms.Overall, the Cambridge Analytica scandal serves as an important case study on the security issues related to social media platforms. It highlights the need for users to be aware of how their personal data is being used, as well as the need for social media companies to take responsibility for protecting user data and preventing its misuse.

2. One recent case in India related to security issues in social media involves the leak of personal data of millions of Indian users from Facebook-owned messaging app, WhatsApp. In October 2020, it was reported that the personal data of around 1.3 million Indian users was among the data leaked as part of a massive data breach that affected over 533 million Facebook users worldwide.The leaked data included phone numbers, email addresses, and other personal information of users, which could potentially be used for identity theft or fraud. The leak raised concerns about the security of personal data on social media platforms, as well as the role of these platforms in protecting users' privacy.In response to the data breach, the Indian government asked WhatsApp to explain the nature of the breach and to take appropriate steps to ensure the privacy and security of users' data. The government also issued a notice to Facebook, WhatsApp's parent company, seeking information about the breach and the measures taken to prevent such incidents in the future. The incident highlights the need for social media platforms to take stronger measures to protect users' personal data and ensure their privacy and security. It also underscores the importance of government oversight and regulation to hold social media companies accountable for any security breaches or violations of users' rights.
3. One case study related to security issues in social media in Assam is the 2018 incident where a rumour circulated on social media platforms about child abductors in the state. The rumour caused widespread panic and led to the lynching of several innocent people by mobs who

believed they were child abductors.The rumour began to circulate on social media platforms, including Facebook and WhatsApp, in late May 2018. The rumour claimed that a group of child abductors were active in the state and were kidnapping children for organ harvesting. The rumour quickly spread throughout the state, and people began to share it widely on social media.As the panic and fear grew, mobs began to form and attack anyone they suspected of being a child abductor. Several innocent people were beaten to death, including two men who were traveling in a car and were mistaken for child abductors.The state government and police authorities quickly moved to quell the violence and dispel the rumours. They issued warnings on social media, urging people not to believe or spread the false rumours. They also arrested several people who were involved in spreading the rumours and inciting violence. The incident highlights the potential dangers of social media and the need for responsible use. False information can spread rapidly on social media platforms, leading to panic and violence. It is important for individuals and authorities to be aware of the potential for false information to spread and take steps to prevent it from doing so.The incident also highlights the need for social media companies to take responsibility for the content that is shared on their platforms. While some companies have taken steps to combat false information and hate speech on their platforms, more needs to be done to ensure that social media is a safe and responsible space for all users.



CHECK YOUR PROGRESS

5. What is the importance of adjusting your content according to your audience on social media?
6. Why is it important to be mindful of the personal information you share on social media?



ACTIVITY

1. Search for a case involving an issue related to social media security and write something down about it.



8.9 LET US SUM UP

- Social media security issues include privacy, cyberbullying, identity theft, malware, and fake accounts.
- Both social media platforms and users should take steps to address these issues, including implementing security measures and promoting responsible use of social media.
- Reporting offensive content promptly and with specific details while understanding the platform's policies is an effective way to keep online spaces safe and inclusive.
- It's important to avoid retaliatory behaviour and understand the limitations of the reporting and flagging process, while also promoting respectful and positive online interactions.
- The publication of offensive material on social media can have serious consequences and laws governing this area can vary depending on the country or jurisdiction.
- It's important to understand the legal framework and definitions of offensive material in your country or jurisdiction to avoid unintentional violations.
- The impact of offensive material on others, particularly vulnerable or marginalized communities, should be considered before publishing content.
- Seeking legal advice when unsure about the legality of publishing certain content can help ensure compliance with local laws.
- Social media companies also have a responsibility to enforce their own community guidelines and policies to prevent the publication of offensive material on their platforms.

- Social media has become an integral part of our daily lives, and it is important to use it responsibly and effectively.
- Best practices for the use of social media include being aware of your audience, thinking before you post, being respectful, protecting your privacy, staying informed, giving credit where it's due, and using social media for positive purposes.



8.10 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: Some main issues with social media security include: privacy breaches, hacking, phishing, identity theft, cyberbullying, and online harassment.

Ans to Q No 2: Some key points to consider when reporting or flagging offensive content on social media include: being specific about the content in question, providing evidence or screenshots, reporting to the appropriate channels, and being aware of the platform's community guidelines and policies.

Ans to Q No 3: Some general points to consider include understanding the local laws, being mindful of the impact of your content, and avoiding hate speech or discriminatory language.

Ans to Q No 4: International agreements and frameworks that provide guidance include the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Rabat Plan of Action on the prohibition of advocacy of national, racial, or religious hatred.

Ans to Q No 5: Adjusting your content according to your audience is important because what might be appropriate for one audience may not be appropriate for another.

Ans to Q No 6: It is important to be mindful of the personal information you share on social media because it can help protect your privacy, and adjusting your privacy settings can limit who can see your posts and personal details.



8.11 FURTHER READINGS

1) Dhir, A., & Dhir, A. (2019). Social media security: Leveraging social networking while mitigating risk. Apress.

2) Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., & Warkentin, M. (2014). Future directions for behavioral information security research. In Behavioral cyber security (pp. 231-244). Springer.

3) Hemsley, J., & Taylor, J. (2019). Social media and crisis communication. Routledge.



8.12 MODEL QUESTIONS

Q1. What are some of the most common security threats on social media?

Q2. How can individuals protect their personal information on social media?

Q3. What steps can businesses take to ensure the security of their social media accounts?

Q4. How do social media platforms themselves work to prevent security breaches and protect user data?

Q5. What are the potential consequences of a security breach on social media, both for individuals and businesses?

Q6. How can social media users identify and avoid phishing and other social engineering attacks?

*** ***** ***

UNIT 9: INTRODUCTION TO E-COMMERCE

UNIT STRUCTURE

9.1 Learning Objectives

9.2 Introduction

9.3 E- Commerce

9.4 Main Components of E-Commerce

9.5 Elements of E-Commerce Security

9.6 E-Commerce Threats

9.7 E-Commerce Security Best Practices.

9.8 Let Us Sum Up

9.9 Answers to Check Your Progress

9.10 Further Readings

9.11 Model Questions

9.1 LEARNING OBJECTIVE

After going through this unit, you will be able to-

- identify diferent types of e-commerce transactions
- analyse the advantages and disadvantages of e-commerce
- evaluate the components of an e-commerce business
- explain the role of security in e-commerce
- develop strategies to improve e-commerce security

9.2 INTRODUCTION

In this unit, we will discuss the main components of E-commerce along with the elements of e-commerce. Various types of E-commerce threats along with best practices related to e-commerce security are also discussed in detail in this unit. In the next unit, are will explore the world of digital payments.

The concept of e-commerce emerged in the 1990s when the internet became widely available to the public. Since then, e-commerce has rapidly grown to become a massive global industry, with millions of businesses using the internet to reach customers, streamline their operations, and expand their market share.

9.3 E-COMMERCE

E-commerce, short for electronic commerce, refers to the buying and selling of goods and services over the internet. In simple terms, it is the process of conducting business transactions electronically through online platforms, including websites, social media, mobile apps, and other digital channels.

E-commerce can be classified into various types based on the types of parties involved, the nature of transactions, and the business models adopted. Some common types of e-commerce include:

- **B2B (Business-to-Business):** This type of e-commerce involves transactions between businesses. In B2B e-commerce, companies sell products or services to other businesses rather than individual customers. Examples:IndiaMART, TradeIndia
- **B2C (Business-to-Consumer):** This type of e-commerce involves transactions between businesses and individual customers. B2C e-commerce is the most common type of e-commerce, and it includes online shopping, travel booking, and other similar services. Examples: Amazon India, Flipkart, Myntra etc
- **C2C (Consumer-to-Consumer):** This type of e-commerce involves transactions between individual customers, such as online auction sites. Example: OLX, Quikr
- **C2B (Consumer-to-Business):** This type of e-commerce involves transactions in which individual customers offer products or services to businesses. Examples: Airbnb, Uber, Ola etc
- **B2G (Business-to-Government):** This type of e-commerce involves transactions between businesses and government entities. Examples: Government e-Marketplace (GeM), Indian Railways E-Procurement System (IREPS)

E-commerce transactions typically involve various stages, including searching for products or services, selecting items, adding them to a virtual shopping cart, making payment, and receiving confirmation and delivery of the purchased items. E-commerce platforms use various payment gateways, including credit cards, debit cards, digital wallets, and online banking.

E-commerce has numerous advantages over traditional brick-and-mortar businesses. It allows businesses to reach a broader customer base, expand their market reach, reduce operational costs, and offer 24/7 services. Customers can also enjoy the convenience of shopping from anywhere at any time, accessing a broader range of products and services, and comparing prices across different platforms.

However, e-commerce also poses several challenges, including cybersecurity threats, fraud, and data breaches. Additionally, businesses must invest in robust e-commerce infrastructure, including websites, mobile apps, and secure payment gateways.

In conclusion, e-commerce is a revolutionary way of conducting business that has transformed the global business landscape. It has enabled businesses to reach more customers, streamline operations, and expand their market share, while also offering customers greater convenience and access to a broader range of products and services.

9.4 MAIN COMPONENTS OF E-COMMERCE

Electronic commerce, or e-commerce, refers to the buying and selling of products or services over the internet. E-commerce has revolutionized the way businesses operate, providing a new platform for conducting transactions, increasing efficiency, and reaching new markets. The main components of e-commerce include:

1. **Website or Online Store:** A website or online store is the digital storefront for an e-commerce business. This is where customers can browse products or services, read descriptions, view prices, and make purchases. The website must be easy to navigate, visually appealing, and secure to ensure a positive user experience.
2. **Shopping Cart:** A shopping cart is a software application that enables customers to add items to their virtual shopping cart and proceed to checkout when they are ready to make a purchase. The shopping cart also calculates the total cost of the purchase, including any taxes and shipping fees.

3. **Payment Gateway:** A payment gateway is an online service that enables e-commerce businesses to accept payments from customers. It securely processes credit card, debit card, and other electronic payments, and verifies that the funds are available before completing the transaction. Popular payment gateways include Paytm, Razorpay, and CCAvenue etc.
4. **Logistics and Fulfilment:** Logistics and fulfilment refer to the process of storing, packaging, and shipping products to customers. E-commerce businesses must have efficient logistics and fulfilment systems in place to ensure that products are delivered to customers in a timely and cost-effective manner. This includes inventory management, order fulfillment, and shipping and tracking.
5. **Customer Relationship Management (CRM):** Customer relationship management (CRM) is the practice of managing interactions with customers throughout the customer journey. In e-commerce, this includes managing customer data, tracking customer behavior, and providing personalized recommendations and promotions. A robust CRM system can help e-commerce businesses build loyalty and increase customer retention.
6. **Security:** Security is a critical component of e-commerce. Customers must feel confident that their personal and financial information is safe when making online purchases. E-commerce businesses must use secure sockets layer (SSL) encryption, two-factor authentication, and other security measures to protect customer data from hackers and other malicious actors.

In conclusion, the main components of e-commerce include a website or online store, a shopping cart, a payment gateway, logistics and fulfillment, customer relationship management, and security. Each component plays a critical role in the success of an e-commerce business, and businesses must ensure that each component is functioning effectively to provide a positive user experience and maximize sales.



CHECK YOUR PROGRESS

Q1. What is e-commerce?

Q2. What are the main types of e-commerce?

Q3. What are the main components of e-commerce?

Q4. What are some advantages of e-commerce?

9.5 ELEMENTS OF E-COMMERCE SECURITY

E-commerce security is a crucial aspect of any online business that accepts payments from customers. With the increasing number of online transactions, it is vital to ensure that sensitive information such as personal and financial data is protected from malicious actors. Here are the key elements of e-commerce security:

- **Secure Socket Layer (SSL) Certificate:** SSL is a security protocol that encrypts data transmitted between a web server and a user's browser. An SSL certificate is a digital certificate that verifies the identity of the website and encrypts data transmitted between the website and the user's browser. SSL is critical for securing online transactions and preventing data breaches.
- **Two-Factor Authentication:** Two-factor authentication (2FA) is an additional layer of security that requires users to provide two forms of identification to access their accounts. This can include a password and a unique code sent to the user's phone or email. 2FA helps prevent unauthorized access to user accounts, reducing the risk of fraud and data breaches.
- **Payment Gateway Security:** Payment gateway security is critical for securing online transactions. Payment gateways should be PCI DSS (Payment Card Industry Data Security Standard) compliant, which means they meet specific security standards set by the payment card industry. Payment gateways should also use encryption and tokenization to protect sensitive data such as credit card information.

- **Fraud Detection and Prevention:** E-commerce businesses should have robust fraud detection and prevention systems in place to identify and prevent fraudulent transactions. This can include monitoring transaction patterns, using machine learning algorithms to detect anomalies, and implementing strict verification processes for high-risk transactions.
- **Regular Security Audits and Updates:** Regular security audits and updates are critical for maintaining the security of an e-commerce website. This can include vulnerability scanning, penetration testing, and software updates to address known security issues. Regular security audits and updates can help identify and address potential security vulnerabilities before they are exploited by hackers.

In conclusion, e-commerce security is critical for protecting user data and preventing fraud and data breaches. The key elements of e-commerce security include SSL certificates, two-factor authentication, payment gateway security, fraud detection and prevention, and regular security audits and updates. E-commerce businesses should prioritize security and implement these elements to ensure the safety and security of their customers' data.

9.6 E-COMMERCE THREATS

E-commerce has become an integral part of our daily lives, and it has brought convenience to the way we shop and transact online. However, with the growth of e-commerce, there has also been a corresponding increase in e-commerce threats. These threats can compromise the security of online transactions, steal sensitive data, and cause significant financial losses. Here are the most common e-commerce threats that businesses and users should be aware of:

Malware and Phishing:

Malware and phishing attacks are among the most common e-commerce threats. Malware refers to software designed to infiltrate or damage computer systems, while phishing refers to fraudulent attempts to

obtain sensitive information such as passwords and credit card details. Hackers can use malware and phishing attacks to steal sensitive data and compromise the security of online transactions.

SQL Injection:

SQL injection is a type of attack that targets websites that use SQL databases. Hackers can use SQL injection attacks to inject malicious code into a website's database and gain access to sensitive data, such as customer information and credit card details.

DDoS Attacks:

Distributed Denial of Service (DDoS) attacks are a type of cyber attack that aims to overwhelm a website with traffic, making it unavailable to legitimate users. DDoS attacks can be used to disrupt e-commerce websites and prevent users from making online transactions.

Payment Fraud:

Payment fraud is a significant threat to e-commerce businesses. Hackers can use stolen credit card information to make fraudulent purchases or transfer money from customer accounts. Payment fraud can cause significant financial losses and damage the reputation of e-commerce businesses.

Account Takeover:

Account takeover occurs when a hacker gains access to a user's account and takes control of it. Account takeover can be used to steal sensitive information, make fraudulent purchases, and compromise the security of online transactions.

To protect against these e-commerce threats, businesses should implement robust security measures, such as SSL certificates, two-factor authentication, and fraud detection and prevention systems. Users should also take precautions, such as using strong passwords, keeping their software up to date, and avoiding suspicious websites and emails. E-

commerce businesses and users should be vigilant and proactive in protecting against e-commerce threats to ensure the safety and security of online transactions.

9.7 E-COMMERCE SECURITY BEST PRACTICES

E-commerce security is a critical aspect of any online business that accepts payments from customers. Implementing best practices for e-commerce security can help prevent data breaches, protect sensitive information, and ensure the safety and security of online transactions. Here are some best practices for e-commerce security:

1. **Implement Strong Password Policies:** E-commerce businesses should require users to create strong passwords that are difficult to guess. Passwords should be at least eight characters long and include a combination of letters, numbers, and special characters. Businesses should also implement password expiration policies and two-factor authentication to provide an additional layer of security.
2. **Use Secure Payment Gateways:** E-commerce businesses should use secure payment gateways that are PCI DSS compliant. Payment gateways should encrypt sensitive information such as credit card details to prevent data breaches and fraud.
3. **Keep Software Up to Date:** E-commerce businesses should regularly update their software and systems to ensure they are protected against known security vulnerabilities. This includes updating web servers, content management systems, and payment gateways.
4. **Regular Security Audits:** E-commerce businesses should conduct regular security audits to identify potential vulnerabilities and address them before they can be exploited. This includes vulnerability scanning, penetration testing, and code review.
5. **Monitor Transactions:** E-commerce businesses should monitor transactions for suspicious activity, such as unusual payment amounts or delivery addresses. This can help identify potential fraud and prevent unauthorized transactions.

6. **Educate Employees:** E-commerce businesses should provide regular training to employees on best practices for e-commerce security. This can include teaching employees how to identify and prevent phishing attacks, how to create strong passwords, and how to handle sensitive information.

In conclusion, implementing best practices for e-commerce security is critical for protecting the sensitive information of customers and ensuring the safety and security of online transactions. E-commerce businesses should implement strong password policies, use secure payment gateways, keep software up to date, conduct regular security audits, monitor transactions, and educate employees on e-commerce security best practices. By following these best practices, businesses can prevent data breaches and ensure the trust and loyalty of their customers.



CHECK YOUR PROGRESS

Q5. What is an SSL certificate?

Q6. What is a common e-commerce threat?

Q7. What is a best practice for e-commerce security?

9.8 LET US SUM UP

- E-commerce, or electronic commerce, is the buying and selling of goods and services over the internet.
- E-commerce emerged in the 1990s and has rapidly grown into a massive global industry.
- There are various types of e-commerce, including B2B, B2C, C2C, C2B, and B2G.
- E-commerce transactions involve stages like searching for products, adding them to a cart, making payments, and receiving confirmation and delivery.
- Payment gateways like credit cards, debit cards, digital wallets, and

online banking are commonly used in e-commerce.

- E-commerce offers several advantages, such as reaching a broader customer base, reducing operational costs, and offering 24/7 services.
- E-commerce also poses several challenges, including cybersecurity threats, fraud, and data breaches.
- The main components of e-commerce include a website or online store, shopping cart, payment gateway, logistics and fulfillment, CRM, and security.
- A website or online store is the digital storefront for an e-commerce business, where customers can browse products and make purchases.
- A shopping cart is a software application that enables customers to add items to their virtual shopping cart and proceed to checkout.
- Payment gateways enable e-commerce businesses to securely accept payments from customers.
- Logistics and fulfillment refer to the process of storing, packaging, and shipping products to customers.
- CRM involves managing customer data, tracking behavior, and providing personalized recommendations and promotions.
- Security measures like SSL encryption, two-factor authentication, and secure servers are critical for protecting customer data.
- Overall, e-commerce has transformed the global business landscape, enabling businesses to reach more customers and streamline operations, while also offering customers greater convenience and access to a broader range of products and services.



9.9 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q No 1: E-commerce is the buying and selling of goods and services over the internet

Ans to Q No 2: The main types of e-commerce are B2B, B2C, C2C, C2B, and B2G

Ans to Q No 3: The main components of e-commerce are a website or online store, a shopping cart, a payment gateway, logistics and fulfilment, customer relationship management, and security

Ans to Q No 4: E-commerce allows businesses to reach a broader customer base, expand their market reach, reduce operational costs, and offer 24/7 services, while customers can enjoy convenience and access to a broader range of products and services.

Ans to Q No 5: A digital certificate that encrypts data transmitted between a website and a user's browser.

Ans to Q No 6: Malware and phishing attacks.

Ans to Q No 7: Implement strong password policies.



9.10 FURTHER READINGS

1) Field, A. P. (2018). An adventure in statistics: The reality enigma. Sage.

2) Cohen, J. (1992). A power primer. Psychological Bulletin, 112(1), 155-159.



9.11 MODEL QUESTIONS

Q1. What are the different types of e-commerce and how do they differ from each other in terms of the parties involved and the nature of transactions?

Q2. What are the main components of e-commerce, and how do they work together to create a seamless online shopping experience for customers?

Q3. What are the advantages and disadvantages of e-commerce for businesses, and how can businesses overcome the challenges associated with conducting transactions online?

Q4. What are the key security concerns associated with e-commerce, and how can businesses ensure that their customers' personal and financial data is protected?

Q5. How has e-commerce transformed the global business landscape, and what impact has it had on traditional brick-and-mortar businesses?

*** ***** ***

UNIT 10: INTRODUCTION TO DIGITAL PAYMENTS

UNIT STRUCTURE

10.1 Learning Objectives

10.2 Introduction

10.3 Digital Payments

- 10.3.1 Importance of Digital Payments
- 10.3.2 History of Digital Payments
- 10.3.3 Components of Digital Payments
- 10.3.4 Stakeholders in Digital Payments

10.4 Modes of Digital Payments

- 10.4.1 Debit Card
- 10.4.2 Credit Card
- 10.4.3 Unified Payment Interface (UPI)
- 10.4.4 e-Wallets
- 10.4.5 Unstructured Supplementary Service Data (USSD)
- 10.4.6 Aadhaar-enabled Payments

10.5 Let us Sum Up

10.6 Answer to Check Your Progress

10.7 Further Readings

10.8 Model Questions

10.1 LEARNING OBJECTIVES

After going through this unit, the learners will be able to :

- understand the importance of digital payments in the modern economy and their impact on financial transactions.
- analyze the history of digital payments and their evolution over time.
- identify the components of digital payments, including the technologies and processes involved in digital transactions.
- explain the different stakeholders involved in digital payments, including customers, merchants, payment service providers, and regulatory authorities.

- describe the various modes of digital payments, including debit cards, credit cards, UPI, e-wallets, USSD, and Aadhaar-enabled payments.

10.2 INTRODUCTION

Digital payments refer to electronic transactions that allow customers to make purchases, transfers, or payments without the need for physical cash.

Digital payments have become an essential aspect of our daily lives due to their convenience, speed, and security. With the increasing use of technology, digital payment methods have become a popular choice for transactions, especially during the COVID-19 pandemic, where contactless payment methods had become a necessity.

This unit covers the fundamental concepts of digital payments, including its history, importance, and components. It also delves into the different modes of digital payments, such as banking cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), and Aadhaar enabled payments.

By the end of this unit, you will have a clear understanding of digital payments, their impact on the economy, and the various modes of digital payments available for individuals and businesses. You will also be equipped with the knowledge required to make informed decisions about which digital payment method is best suited for your needs.

10.3 DIGITAL PAYMENTS

Digital payments refer to electronic transactions that allow individuals and businesses to transfer money, pay bills, and make purchases online without the need for physical cash. In digital payments, money is transferred electronically between bank accounts or through digital wallets. The use of digital payments has become increasingly popular due to their convenience, speed, and security. They have revolutionized the way we make transactions, making it easier for individuals and businesses to conduct financial

transactions anytime and anywhere. With the rise of technology, digital payments have become an essential aspect of our daily lives.

10.3.1 Importance Of Digital Payments

Digital payments play a vital role in our modern economy. Here are some of the reasons why digital payments are important:

(a) Convenience: Digital payments provide a convenient way for individuals and businesses to make transactions without the need for physical cash or checks.

(b) Speed: Digital payments are processed almost instantly, allowing for faster transactions and payments.

(c) Security: Digital payments are more secure than traditional methods of payment, such as cash and checks, as they use encryption and authentication to protect personal and financial information.

(d) Cost-Effective: Digital payments are cost-effective, as they eliminate the need for manual processing, reducing the costs associated with paper-based transactions.

(e) Financial Inclusion: Digital payments enable individuals who do not have access to traditional banking systems to participate in the digital economy, promoting financial inclusion.

(f) Increased Efficiency: Digital payments automate many processes and provide real-time transaction information, making them more efficient than traditional payment methods.

Overall, digital payments have transformed the way we conduct transactions, making them faster, more secure, and more efficient. They are an essential component of our modern economy, promoting financial inclusion and driving economic growth.

10.3.2 History Of Digital Payments

The history of digital payments can be traced back to the early 1970s when the first electronic fund transfer system, known as

Electronic Funds Transfer (EFT), was introduced. However, it wasn't until the late 1990s and early 2000s that digital payments began to gain popularity with the rise of the internet and e-commerce.

In 1998, PayPal was founded, offering a new way for individuals and businesses to make online payments. In 2003, the first mobile payment system, M-Pesa, was launched in Kenya, allowing individuals to send and receive money using their mobile phones.

The introduction of credit and debit cards also played a significant role in the development of digital payments. In the 1950s, the first credit card, known as the Diner's Club Card, was introduced, followed by the first debit card, the ATM card, in the 1960s.

Today, digital payments have become an essential part of our daily lives, with a variety of payment methods available, including online banking, e-wallets, mobile payments, and contactless payments. The ongoing development of new technologies and payment methods continues to drive the growth of digital payments, making them an increasingly important part of our modern economy.

10.3.3 Components of Digital Payments

The components of digital payments include:

(a) Payment Gateway: A payment gateway is a software service that enables merchants to securely process online transactions. It facilitates the transfer of information between the merchant's website or mobile application and the bank or payment processor.

(b) Digital Wallets: Digital wallets are virtual accounts that store payment card information and other payment methods. They allow users to make payments easily and securely using their smartphones or other digital devices.

(c) Point of Sale (POS) Terminals: POS terminals are used by merchants to accept card payments at their physical stores or outlets. They can be standalone devices or integrated into cash registers.

(d) Payment Processors: Payment processors are companies that process and authorize payments between merchants and their customers. They handle the technical aspects of payment processing, such as encryption and fraud detection, and facilitate the transfer of funds between banks.

(e) Mobile Payments: Mobile payments are transactions made using mobile devices, such as smartphones or tablets. They can be made using a variety of technologies, including Near Field Communication (NFC), QR codes, or mobile apps.

(f) Electronic Funds Transfer (EFT): EFT is a system for transferring funds electronically between bank accounts. It allows individuals and businesses to make payments and receive payments directly into their bank accounts.

Overall, the components of digital payments work together to provide a seamless and secure experience for users, making it easier to make transactions online and in-person.

10.3.4 Stakeholders in Digital Payments

There are several stakeholders involved in digital payments, including:

(a) Consumers: Consumers are the end-users of digital payments. They use digital payment methods to make transactions, whether online or in-person.

(b) Merchants: Merchants are the businesses or individuals who accept digital payments for their goods or services. They may use various payment methods, such as payment gateways, mobile payments, or POS terminals, to receive payments.

(c) Banks: Banks play a critical role in digital payments as they provide the infrastructure to process transactions. They provide payment gateways, merchant accounts, and other financial services to facilitate the transfer of funds.

(d) Payment Processors: Payment processors are companies that facilitate the transfer of funds between banks and merchants.

They handle the technical aspects of payment processing, such as encryption and fraud detection, to ensure secure transactions.

(e) Regulators: Regulators are responsible for ensuring that digital payments comply with applicable laws and regulations. They establish rules and guidelines to protect consumers, merchants, and other stakeholders.

(f) Technology Providers: Technology providers develop and maintain the software and hardware necessary for digital payments to work. They may provide payment gateways, mobile apps, POS terminals, or other digital payment solutions.



CHECK YOUR PROGRESS

Q1. Choose the correct option:

A. What is the main advantage of digital payments over traditional payment methods?

(a) Faster transactions

(b) Increased efficiency

(c) More secure

(d) All of the above

B. What was the first electronic fund transfer system introduced in the 1970s?

(a) PayPal

(b) M-Pesa

(c) EFT

(d) Diner's Club Card

C. Which of the following is not a component of digital payments?

(a) Payment Gateway

(b) POS Terminals

(c) Digital Coupons

(d) Mobile Payments

D. Who are the stakeholders involved in digital payments?
   (a) Consumers, Merchants, Banks, Payment Processors, Regulators, Technology Providers
   (b) Consumers, Sellers, Buyers, Banks, Technology Providers, Payment Processors
   (c) Consumers, Sellers, Banks, Payment Processors, Technology Providers, Advertisers
   (d) Consumers, Banks, Payment Processors, Regulators, Technology Providers, Advertisers

E. What is the significance of digital payments in promoting financial inclusion?
   (a) They allow individuals without access to traditional banking systems to participate in the digital economy
   (b) They provide faster transactions for individuals and businesses
   (c) They are more cost-effective than traditional payment methods
   (d) None of the above

10.4 MODES OF DIGITAL PAYMENTS

Digital payments are electronic transactions that enable consumers to purchase goods and services without the use of physical cash. There are several modes of digital payments available today. In this section, we will briefly discuss various digital payment modes. Here are some of the most common modes of digital payments:

(a) **Mobile Payments:** Mobile payments allow customers to make payments through their mobile phones. This mode of payment includes mobile wallets like Apple Pay, Google Pay, and Samsung Pay, which enable customers to store their credit card information securely on their mobile devices.

(b) **Online Banking:** Online banking allows customers to pay bills and transfer funds online. Customers can use online banking services provided by their banks to make payments.

(c) **E-Wallets:** E-wallets are digital wallets that enable customers to store their money electronically. Customers can add money to their e-wallets using debit or credit cards, bank transfers, or other modes of payment.

(d) **Cryptocurrencies:** Cryptocurrencies like Bitcoin and Ethereum enable customers to make payments without the need for a financial intermediary. Cryptocurrencies are decentralized and use blockchain technology to facilitate secure and transparent transactions.

(e) **Point of Sale (POS) Systems:** POS systems are used by merchants to accept payments from customers. These systems enable customers to pay using credit or debit cards, mobile wallets, or other digital payment methods.

(f) **Online Marketplaces:** Online marketplaces like Amazon and eBay provide customers with a range of payment options, including credit and debit cards, mobile payments, and digital wallets.

10.4.1 Debit Card

Digital payments through a debit card are a popular mode of electronic transactions. Let us look at how it works:

- Firstly, a debit cardholder needs to have an account with a bank that issues the debit card.
- The debit card must be linked to the account and activated for online transactions.
- When making a purchase, the customer needs to select the debit card option as the mode of payment.
- The customer will then be required to enter the debit card number, expiration date, and CVV code (the three-digit security code found on the back of the card).
- The customer will then be prompted to enter the amount to be paid, and the transaction will be processed.
- In some cases, the customer may be required to enter a one-time password (OTP) sent to their registered mobile number for added security.

- Once the transaction is approved, the customer's bank account will be debited with the amount of the purchase.

Digital payments through a debit card are convenient and secure, as they allow customers to make transactions without carrying cash or checks. Additionally, many banks offer rewards and cashback on debit card transactions, making them a popular mode of payment.

10.4.2 Credit Card

Digital payments through credit cards are a popular mode of payment for purchasing goods and services online or at a point of sale. Let us look at the step-by-step procedure on how to make digital payments through a credit card:

(a) Use of Credit Card for Online Transaction:

Step 1: Choose a website or app: First, you need to choose the website or app where you want to make the payment. Ensure that the website or app is secure and trusted.

Step 2: Add items to cart: Browse the products or services and add them to your cart.

Step 3: Checkout: Once you have added all the items to your cart, proceed to checkout.

Step 4: Select payment method: Select "credit card" as your payment method.

Step 5: Enter credit card details: Enter your credit card details, including the card number, expiry date, and CVV code. Ensure that you enter the correct information.

Step 6: Verify transaction: Verify the transaction details, including the total amount and the products or services you are purchasing.

Step 7: Confirm payment: Once you have verified the transaction details, confirm the payment. You may be required to enter a One-Time Password (OTP) or other security codes to confirm the payment.

Step 8: Wait for confirmation: After you have confirmed the payment, wait for a few seconds for the transaction to be processed. You will receive a confirmation message once the transaction is successful.

Step 9: Check credit card statement: Finally, check your credit card statement to ensure that the transaction has been processed correctly and that the amount has been deducted from your account.

(b) Use of Credit Card at a Point of Sale (POS):

Let us now look at a step-by-step guide for making a digital payment using a credit card at a point of sale (POS):

Step 1: Choose the items: Start by choosing the items you want to purchase from the store.

Step 2: Head to the checkout: Once you have all the items you want, head to the checkout counter.

Step 3: Enter the purchase amount: The cashier will tell you the total amount you need to pay. Enter this amount into the credit card machine or terminal.

Step 4: Swipe or insert your card: You can then swipe your credit card or insert it into the terminal. If you're using a chip-enabled card, you may be asked to leave the card in the terminal until the transaction is complete.

Step 5: Enter your PIN or sign: You may be asked to enter your PIN or sign a receipt to authorize the transaction.

Step 6: Wait for approval: The credit card machine will then communicate with your bank to approve the transaction. Which can take a few seconds.

Step 7: Take your card and receipt: Once the transaction is approved, the credit card machine may print out a receipt.

10.4.3 Unified Payment Interface (UPI)

Unified Payment Interface (UPI) is a payment system developed by the National Payments Corporation of India (NPCI) that facilitates instant fund transfer between two bank accounts through a mobile device. It is an inter-bank transfer system that allows users to transfer funds using a Virtual Payment Address (VPA) or bank account number and IFSC code.

UPI was launched in 2016 and has since become a popular payment method in India. It allows users to transfer funds 24/7 and 365 days a year, without the need for any bank account details or OTPs. UPI also offers several value-added services like bill payments, mobile recharges, and ticket booking, making it a convenient payment option for consumers.

UPI transactions are processed in real-time, and the funds are credited to the beneficiary's account immediately. The platform supports transactions up to INR 1 lakh per transaction, making it suitable for both small and large transactions.

How to Use UPI?To use UPI, users need to download a UPI-enabled mobile app from their bank or a third-party provider. They need to link their bank account to the app and create a VPA, which serves as their unique identifier for UPI transactions. Once the VPA is created, users can initiate a transaction by entering the beneficiary's VPA or bank account number and IFSC code and authorizing the payment through a UPI PIN.

UPI has revolutionized the payment landscape in India by making fund transfers quick, convenient, and secure. It has played a significant role in promoting digital payments in the country and has brought millions of unbanked and underbanked people into the formal banking system.

There are various types of UPI transactions that one can perform:

- **Peer-to-Peer (P2P) Transactions:** This is the most common type of UPI transaction, where one can transfer funds from their bank account to another person's bank account. This type of

transaction is usually used for person-to-person money transfers, splitting bills, or paying for services.

- **Peer-to-Merchant (P2M) Transactions:** This type of UPI transaction is used to pay for goods and services to registered merchants using their UPI ID. This type of transaction is becoming increasingly popular in India as it eliminates the need for cash payments.
- **Merchant-to-Peer (M2P) Transactions:** This type of UPI transaction is used by merchants to refund money to their customers. The merchant initiates the transaction by entering the customer's UPI ID and the amount to be refunded.
- **Merchant-to-Merchant (M2M) Transactions:** This type of UPI transaction is used by registered merchants to transfer funds between their bank accounts. This type of transaction is commonly used for business-to-business payments, supplier payments, and other commercial transactions.
- **Bill Payments:** UPI also enables users to pay their utility bills, including electricity, water, gas, and phone bills. Users can make these payments by selecting the appropriate biller from the list of billers available on their UPI app.
- **Donations:** UPI also enables users to donate to registered charities and non-profit organizations by selecting the appropriate option on their UPI app.

These are the various types of UPI transactions that are currently available in India. UPI has revolutionized the way people make payments in India and has made it easier, faster, and more convenient to transfer funds between bank accounts.

10.4.4 e-Wallets

e-Wallets, also known as digital wallets or mobile wallets, are a type of electronic payment system that allows users to store their payment card information securely in a digital form. These wallets

enable users to make transactions quickly and conveniently without the need to carry physical cash or credit cards.

e-Wallets can be used to make payments for a variety of transactions such as online shopping, bill payments, mobile recharges, and peer-to-peer transfers. Some popular e-wallets are Paytm, Google Pay, PhonePe, Amazon Pay, and PayPal. Let us look at some of them in detail.

(a) BHIM

BHIM (Bharat Interface for Money) is a UPI-based payment app developed by the National Payments Corporation of India (NPCI). It allows us to make instant and secure transactions directly from the bank account using our mobile device.

To use BHIM UPI, we need to follow these steps:

Step 1: We need to download and install the BHIM UPI app from the Google Play Store or Apple App Store.

Step 2: We need to register for BHIM UPI by entering the mobile number linked to the bank account and creating a UPI PIN.

Step 3: We need to the link the bank account(s) to the BHIM UPI app by providing the required details.

Step 4: Once the bank account(s) are linked, we can start making transactions using BHIM UPI.

Step 5: To make a payment, select the 'Send Money' option, enter the recipient's UPI ID or bank account details, enter the amount you want to send, and confirm the transaction using the UPI PIN.

Step 6: To receive money, share your UPI ID with the sender or use the 'Request Money' option in the app.

Step 7: We can also check your transaction history, manage our linked bank accounts, and set transaction limits using the BHIM UPI app.

We should remember to always keep our UPI PIN safe and never share it with anyone. BHIM UPI is a secure and convenient way to make digital payments.

(b) Google Pay

Google Pay is one of the most popular UPI services in India. It is available on both Android and iOS platforms and allows users to make payments,recharge mobile phones and pay bills.

Let us look at a step-by-step procedure on how to use Google Pay:

Step 1: We need to download and install the Google Pay app on your smartphone from the Google Play Store or Apple App Store.

Step 2: Sign in to our Google account or create a new one if we don't have one.

Step 3: Add a payment method to our Google Pay account. We can either link a credit or debit card, add a bank account, or set up a payment gateway account.

Step 4: Once the payment method is linked, you can use Google Pay to make payments at merchants that accept it.

Step 5: To make a payment using Google Pay, open the app and select the "Pay" option.

Step 6: We need to hold our phone near the payment terminal or scan the QR code at the merchant's checkout counter.

Step 7: Enter the amount you want to pay and verify the payment details.

Step 8: Confirm the payment by entering your Google Pay PIN or using your device's biometric authentication.

Step 9: Once the payment is processed, you'll receive a notification from Google Pay with the transaction details.

(c) Paytm

Paytm is another popular UPI service in India. It is a mobile wallet and payments platform that enables users to send and receive money and pay bills.

To make payments through Paytm, we need to follow the steps below:

Step 1: We need to download the Paytm app from the Google Play Store or Apple App Store and sign up for a Paytm account by entering the mobile number, email ID, and setting up a password.

Step 2: Add money to the Paytm wallet using a debit card, credit card, or net banking. Alternatively, we can link our bank account to our Paytm account and transfer funds directly from our bank account to our Paytm wallet.

Step 3: To make a payment, select the 'Pay' option on the Paytm app's home screen.

Step 4: Enter the mobile number or UPI ID of the person or business you want to pay.

Step 5: We need to enter the amount you want to pay and select the mode of payment - either Paytm wallet, linked bank account, or credit/debit card.

Step 6: Review the transaction details, and if everything looks good, tap on the 'Proceed to Pay' button.

Step 7: If you are paying through a linked bank account or credit/debit card, you may need to enter your card or bank account details and authenticate the transaction using OTP or other methods of verification.

Step 8: Once the payment is successful, you will receive a confirmation message on the app and via SMS.

In addition to the above steps, Paytm also offers a range of other services like bill payments, recharge, booking movie tickets, flight tickets, and more.

(d) PhonePe

PhonePe is a UPI-based digital payments platform that allows users to transfer money, pay bills, and recharge mobile phones. It is available on both Android and iOS platforms.

To make payments through PhonePe, you can follow these simple steps:

Step 1: We need to download the PhonePe app from the Google Play Store or Apple App Store and sign up for a PhonePe account by entering your mobile number, email ID, and setting up a password.

Step 2: Link our bank account(s) with the PhonePe app. You can do this by providing your bank account details, or using UPI ID, if you have already registered for UPI.

Step 3: To make a payment, select the 'Send' option on the PhonePe app's home screen.

Step 4: Enter the mobile number or UPI ID of the person or business you want to pay.

Step 5: Enter the amount you want to pay and select the mode of payment - either PhonePe wallet or linked bank account.

Step 6: Review the transaction details, and if everything looks good, tap on the 'Send' button.

Step 7: If you are paying through a linked bank account, you may need to enter your UPI PIN and authenticate the transaction using OTP or other methods of verification.

Step 8: Once the payment is successful, you will receive a confirmation message on the app and via SMS.

In addition to the above steps, PhonePe also offers a range of other services like bill payments, recharge, booking movie tickets, flight tickets, and more.

(e) Amazon Pay

Amazon Pay is a digital wallet service that allows users to make online payments and transfer money to other Amazon Pay users. It is available on both Android and iOS platforms.

To make payments through Amazon Pay, you can follow these steps:

Step 1: Log in to your Amazon account or create a new one if you don't already have one.

Step 2: Add money to your Amazon Pay account using a debit card, credit card, or net banking. Alternatively, you can link your bank account to your Amazon Pay account and transfer funds directly from your bank account to your Amazon Pay balance.

Step 3: To make a payment, select the 'Amazon Pay' option on the payment page of the merchant you are transacting with.

Step 4: Enter your Amazon Pay login credentials and select the option to pay using your Amazon Pay balance.

Step 5: If you don't have sufficient balance in your Amazon Pay account, you can select the option to pay using a linked credit or debit card, net banking, or UPI.

Step 6: Enter the amount you want to pay and review the payment details.

Step 7: If everything looks good, click on the 'Pay Now' button.

Step 8: Once the payment is successful, you will receive a confirmation message on the merchant's website as well as in your email and Amazon account.

In addition to the above steps, Amazon Pay also offers a range of other services like bill payments, mobile recharges, and money transfers.

Precautions for using e-wallet

Here are some precautions we can take to keep our e-wallet safe:

- **Use strong passwords:** Use a strong password that is difficult to guess and avoid using the same password for different accounts.
- **Enable two-factor authentication:** Many e-wallets offer two-factor authentication which adds an extra layer of security. This ensures that we are the only person who can access our account.
- **Update the app:** Keep the e-wallet app up to date to ensure that we have the latest security features and bug fixes.
- **Avoid using public Wi-Fi:** Avoid using public Wi-Fi or any other

unsecured networks when accessing your e-wallet account. Hackers can easily intercept your data on unsecured networks.

- **Verify the sender:** Always verify the sender before making any transaction. Fraudsters may send fake messages or emails that appear to be from your e-wallet provider to trick you into sharing your personal information.
- **Use trusted sources:** Only download the e-wallet app from trusted sources like the official app store of your device's operating system.
- **Check transaction history:** Check your transaction history regularly to ensure that there are no unauthorized transactions.
- **Keep your device secure:** Keep your device secure by using a strong password or PIN, and installing antivirus software to protect it from malware and viruses.

By taking these precautions, we can help ensure that our e-wallet is secure and our personal and financial information is protected.

10.4.5 Unstructured Supplementary Service Data (USSD)

Unstructured Supplementary Service Data (USSD) is a protocol used to communicate between a mobile device and a service provider's computer system. It is a session-based, real-time messaging service that allows users to interact with a service provider's computer system through a menu-driven interface, using short codes or "quick codes" that are easy to remember.

USSD messages are usually initiated by the user dialing a short code on their mobile device, followed by a series of numbers or characters that represent the specific service they want to access. The service provider's computer system responds to the request with a menu of options, which the user can navigate through by entering more numbers or characters.

USSD is widely used for a variety of services, including mobile banking, mobile money transfer, and mobile recharge services. It is

particularly popular in developing countries where many people do not have access to smartphones or mobile apps, as USSD can be accessed on even the most basic mobile phones. USSD is also known for its reliability, as it can be used even in areas with poor network coverage or slow internet connectivity.

It allows users to access various services and interact with their mobile network operator by entering a code on their mobile phone.

Let us look at an example of how to use USSD to check our mobile phone balance:

Step 1: Dial *123# from your mobile phone.

Step 2: Press the call button.

Step 3: A message will appear on your phone screen, asking you to choose an option.

Step 4: Choose option 1 to check your account balance.

Step 5: Another message will appear on your phone screen, displaying your current account balance.

This is just one example of how USSD can be used to interact with your mobile network operator. Other common uses of USSD include buying airtime, subscribing to data plans, and transferring funds. USSD is a quick and convenient way to access these services, especially for users who do not have access to the internet or who prefer not to use mobile apps.

10.4.6 Aadhaar-Enabled Payments

Aadhaar-enabled Payments is a digital payment system that enables consumers to make transactions using their Aadhaar number and biometric authentication. Aadhaar is a 12-digit unique identification number issued by the Indian government to its residents, and it contains biometric data such as fingerprints and iris scans.

The Aadhaar-enabled Payments system allows users to link their bank accounts to their Aadhaar number and make payments through biometric authentication at merchant establishments or

through online transactions. This system is designed to provide a secure and convenient way for people to make transactions, particularly for those who do not have a smartphone or a debit card.

To use Aadhaar-enabled Payments, users must first link their bank account to their Aadhaar number, which can be done at the bank or through the Aadhaar website. Once the account is linked, users can make payments by providing their Aadhaar number and verifying their identity through biometric authentication at a point-of-sale (POS) terminal or through online transactions.

Aadhaar-enabled Payments have been implemented across India to facilitate financial inclusion and provide a secure and efficient way for people to make payments. This system has been particularly useful in rural areas where traditional banking services are limited, and people may not have access to smartphones or debit cards.



CHECK YOUR PROGRESS

Q2. Choose the correct option:

A. Which of the following is NOT a mode of digital payment?

(a) Mobile payments

(b) Online banking

(c) Cash payments

(d) E-wallets

B. Which of the following is a benefit of using digital payments through debit cards?

(a) They provide a high level of security for transactions

(b) They allow for transactions without carrying cash or checks

(c) They can earn rewards and cashback on transactions

(d) All of the above

C. Which of the following is a step in making a digital payment through credit cards for an online transaction?

(a) Choose a website or app
(b) Swipe or insert your card
(c) Enter the purchase amount
(d) None of the above

D. Which of the following is NOT a benefit of using digital payments through Unified Payments Interface (UPI)?
(a) They offer seamless and instant transactions
(b) They can be used to pay bills and transfer funds
(c) They require a physical card for transactions
(d) They allow for transactions 24/7

E. Which of the following is a step in making a digital payment using a credit card at a point of sale?
(a) Enter credit card details
(b) Verify the transaction details
(c) Add items to cart
(d) None of the above



10.5 LET US SUM UP

- Digital payments are electronic transactions that enable individuals and businesses to transfer money, pay bills, and make purchases online without the need for physical cash.
- Digital payments are important because they offer convenience, speed, security, cost-effectiveness, financial inclusion, and increased efficiency.
- The history of digital payments can be traced back to the early 1970s with the introduction of the Electronic Funds Transfer (EFT) system, but it wasn't until the late 1990s and early 2000s that digital payments began to gain popularity with the rise of the internet and e-commerce.
- The components of digital payments include payment gateways, digital wallets, point of sale (POS) terminals, payment processors, mobile payments, and electronic funds transfer (EFT).
- Types of digital payments include online banking, e-wallets, mobile payments, contactless payments, and peer-to-peer (P2P) payments.

- Debit card and credit card are popular modes of digital payments for online and point of sale transactions.
- Digital payments through debit or credit cards offer convenience and security, and many banks provide rewards and cashback on transactions.
- Unified Payment Interface (UPI) is an inter-bank transfer system developed by NPCI that facilitates instant fund transfer between two bank accounts through a mobile device.
- UPI allows users to transfer funds 24/7 and 365 days a year using a Virtual Payment Address or bank account number and IFSC code, and also offers value-added services like bill payments, mobile recharges, and ticket booking.
- UPI has revolutionized the payment landscape in India by making fund transfers quick, convenient, and secure, and has played a significant role in promoting digital payments.
- e-Wallets are a type of electronic payment system that stores payment card information securely in a digital form.
- e-Wallets allow users to make transactions quickly and conveniently without the need to carry physical cash or credit cards.
- e-Wallets can be used for various transactions such as online shopping, bill payments, mobile recharges, and peer-to-peer transfers.
- Some popular e-Wallets include Paytm, Google Pay, PhonePe, Amazon Pay, and PayPal.
- e-Wallets have made transactions more convenient and secure, especially in today's digital age.
- Aadhaar-enabled Payments is a digital payment system that allows consumers to make transactions using their Aadhaar number and biometric authentication.
- Aadhaar-enabled Payments system is designed to provide a secure and convenient way for people to make transactions, particularly for those who do not have a smartphone or a debit card, and has been particularly useful in rural areas where traditional banking services are limited.



10.6 ANSWER TO CHECK YOUR PROGRESS

Ans.to Q.No.1: A. (d) B. (c) C. (c) D. (a)E. (a)

Ans.to Q.No.2: A.(c) B.(d) C.(a) D.(c) E.(b)



10.7 FURTHER READINGS

1) Cyber Crime Impact in the New Millennium, by R. C Mishra ,Auther Press. Edition 2010.

2) Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by SumitBelapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)

3) Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)

4) Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.

5) Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.

6) Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.

7) Fundamentals of Network Security by E. Maiwald, McGraw Hill.



10.8 MODEL QUESTIONS

Q.1: What are some of the advantages of using digital payments over traditional payment methods?

Q.2: Can you describe the history of digital payments and how they have evolved over time?

Q.3: What are the different components involved in digital payments, and how do they work together to provide a seamless experience?

Q.4: Who are the stakeholders involved in digital payments, and what roles do they play in the process?

Q.5: What are some of the emerging trends in digital payments, and how are they shaping the future of finance?

Q.6: How do digital payments promote financial inclusion, and what are some of the challenges that need to be addressed to ensure equal access to digital financial services?

Q.7: What are digital payments, and how do they differ from traditional payments?

Q.8: What are some of the most common modes of digital payments, and how do they work?

Q.9: What is mobile payment, and what are some popular mobile wallets?

Q.10: How does online banking facilitate digital payments, and what services do banks provide to their customers for online payments?

Q.11: What are e-wallets, and how do they work? What are some popular e-wallets available today?

Q.12: What are cryptocurrencies, and how do they enable customers to make payments without the need for a financial intermediary?

Q.13: What are e-Wallets, and how do they work? Name a few popular e-wallets used in India.

Q.14: What is BHIM UPI, and how can you start using it for making digital payments? Explain the step-by-step procedure to use the BHIM UPI app.

Q.15: What is Google Pay, and how can you use it to make payments at merchants? Explain the step-by-step process to use Google Pay for making payments.

Q.16: What is Paytm, and how can you use it to send and receive money, pay bills, and book movie tickets? Explain the step-by-step procedure to use Paytm for making payments.

Q.17: What is Aadhaar-enabled Payments and how does it work?

Q.18: How does Aadhaar-enabled Payments benefit people in rural areas?

Q.19: What is the process for linking a bank account to an Aadhaar number?

Q.20: How does biometric authentication ensure the security of Aadhaar-enabled Payments?

*** ***** ***

UNIT 11: SECURITY ASPECTS IN DIGITAL PAYMENTS

UNIT STRUCTURE

11.1 Learning Objectives

11.2 Introduction

11.3 Common Frauds in Digital Payments

- 11.3.1 Identity theft and Phishing Scams
- 11.3.2 Unauthorized Transactions and Payment Gateway Frauds
- 11.3.3 Fake Payment Apps and Malware Attacks
- 11.3.4 QR Code Frauds and SIM Swap Frauds

11.4 Preventive Measures for Digital Payment Frauds

- 11.4.1 Safe Browsing Practices and Password Management
- 11.4.2 Two-factor Authentication and Biometric Authentication
- 11.4.3 Avoiding Public Wi-Fi and Using Trusted Payment Gateways
- 11.4.4 Regularly Checking Transaction History and Setting Transaction Alerts

11.5 RBI Guidelines on Digital Payments

- 11.5.1 Overview of RBI's Role in Regulating Digital Payments
- 11.5.2 RBI guidelines on Customer Protection in Digital Transactions
- 11.5.3 Complaint Redressal Mechanisms and Dispute Resolution Procedures

11.6 Payment Settlement Act, 2007

- 11.6.1 Overview of the Payment Settlement Act, 2007
- 11.6.2 Provisions Related to Payment Systems, Payment Gateways, and Payment Settlement
- 11.6.3 Legal Implications of Unauthorized Transactions and Payment Frauds Under the Act

11.7 Let us Sum Up

11.8 Answer to Check Your Progress

11.9 Further Readings

11.10 Model Questions

11.1 LEARNING OBJECTIVES

After going through this unit, the learners will be able to :

- understand the common types of digital payment frauds such as identity theft, phishing scams, unauthorized transactions, fake payment apps, and QR code frauds.
- learn about preventive measures for digital payment frauds, including safe browsing practices, two-factor authentication, avoiding public Wi-Fi, and regularly checking transaction history.
- explore the guidelines provided by the RBI on digital payments, including customer protection, complaint redressal mechanisms, and dispute resolution procedures.
- understand the Payment Settlement Act, 2007, including provisions related to payment systems, payment gateways, and payment settlement, and the legal implications of unauthorized transactions and payment frauds under the Act.

11.2 INTRODUCTION

Digital payments have become increasingly popular in recent years, providing individuals and businesses with a convenient and secure way to conduct financial transactions. However, as the use of digital payments has grown, so has the risk of fraud. This unit provides an overview of the common frauds in digital payments, including identity theft, phishing scams, unauthorized transactions, payment gateway frauds, fake payment apps, QR code frauds, and SIM swap frauds. The unit also explores the preventive measures that can be taken to protect oneself from digital payment frauds, such as safe browsing practices, two-factor authentication, and using trusted payment gateways. Furthermore, this content discusses the role of the Reserve Bank of India (RBI) in regulating digital payments, including its guidelines on customer protection in digital transactions and complaint redressal mechanisms. Finally, the unit provides an overview of the Payment Settlement Act, 2007, its provisions related to payment systems, payment

gateways, and payment settlement, and the legal implications of unauthorized transactions and payment frauds under the Act. After going through this unit, learners will gain a better understanding of digital payment frauds and how to protect themselves from such risks. In the next few units, we will explore digital device security and Wi-Fi security

11.3 COMMON FRAUDS IN DIGITAL PAYMENTS

11.3.1 Identity Theft and Phishing Scams

Identity theft is a type of fraud where someone steals another person's personal information, such as their name, date of birth, Social Security number, or financial information, and uses it to make unauthorized purchases or transactions. Identity theft can have serious consequences for victims, including financial loss, damage to their credit rating, and potential legal and criminal issues.

Phishing scams, on the other hand, are a type of social engineering attack where fraudsters try to trick people into sharing their personal information or payment details through fake websites or emails that appear to be from legitimate sources. Phishing scams often use social engineering tactics, such as creating a sense of urgency or fear to encourage victims to act quickly and without thinking. These scams can be difficult to spot, as they often appear to be legitimate messages from well-known companies or financial institutions.

Both identity theft and phishing scams can be very damaging to individuals and businesses, so it's important to be vigilant and take steps to protect your personal information and financial details. This includes regularly checking your credit report, using strong passwords, being cautious about sharing personal information online, and staying up-to-date on the latest phishing and fraud scams.

11.3.2 Unauthorized Transactions and Payment Gateway Frauds

Unauthorized transactions occur when a person or entity makes a transaction on your behalf without your permission. This could happen if someone gains access to your payment information, such as your credit card number or bank account details, and uses it to make purchases or transfers funds without your knowledge or consent. Unauthorized transactions can lead to financial losses for the victim and can cause significant stress and inconvenience.

Payment gateway frauds, on the other hand, involve fraudulent activities that take place during the payment process. A payment gateway is a technology platform that facilitates online transactions between merchants and customers. Fraudsters can exploit vulnerabilities in the payment gateway system to steal payment information or redirect payments to their own accounts. Some common types of payment gateway frauds include phishing attacks, fake merchant websites, and stolen credit card data.

Both unauthorized transactions and payment gateway frauds can have serious consequences for victims, including financial losses and damage to their credit scores. To prevent these types of fraud, it's important to keep your payment information secure, use reputable payment processors, and monitor your financial accounts regularly for any suspicious activity. If you suspect that you've been a victim of unauthorized transactions or payment gateway frauds, you should contact your bank or financial institution immediately to report the issue and take steps to protect your accounts.

11.3.3 Fake Payment Apps and Malware Attacks

Fake payment apps are fraudulent mobile applications that masquerade as legitimate payment apps but are designed to steal users' personal and financial information. These fake apps can be downloaded from untrusted sources or through phishing attacks, where

users are tricked into downloading the fake app by clicking on a malicious link or email.

Once installed, the fake payment app will ask users to enter their payment information, such as credit card details or bank account numbers, and then use this information to steal money or make unauthorized transactions. Some fake payment apps may also ask for personal information such as login credentials or social security numbers, which can be used for identity theft.

Malware attacks, on the other hand, involve malicious software programs that are designed to infiltrate and damage computer systems or mobile devices. Malware can be spread through email attachments, unsecured websites, or social engineering tactics such as phishing.

Once malware infects a device, it can perform a variety of malicious activities, including stealing sensitive information, hijacking user accounts, and displaying unwanted ads. Malware attacks can be especially dangerous when they target financial information, as they can result in financial losses or identity theft.

To protect against fake payment apps and malware attacks, it's important to only download apps from trusted sources, such as official app stores, and to be cautious when clicking on links or downloading attachments from unknown sources. Users should also keep their devices and software up-to-date with the latest security patches, use strong passwords, and regularly monitor their financial accounts for any suspicious activity.

11.3.4 QR Code Frauds and SIM Swap Frauds

QR code frauds involve the use of fraudulent QR codes that are designed to steal personal and financial information from unsuspecting victims. QR codes are 2D barcodes that can be scanned using a mobile device to quickly access information, such as website URLs or payment information. Fraudsters can create fake QR codes that look like legitimate ones, but instead, they redirect

users to a malicious website or steal personal information from the user's device.

QR code frauds can occur in various forms, such as phishing attacks, where the fraudster sends a fraudulent QR code to the victim through email or social media, or by placing fake QR codes in public places, such as on posters or in public transport.

SIM swap frauds, on the other hand, involve the fraudulent transfer of a victim's mobile phone number to a new SIM card that is controlled by the fraudster. This can happen when the fraudster convinces the victim's mobile service provider to transfer the victim's phone number to a new SIM card, often by posing as the victim or providing fake identification documents.

Once the fraudster gains control of the victim's phone number, they can use it to access the victim's personal and financial accounts that are protected by two-factor authentication. This can allow them to bypass security measures and make unauthorized transactions or steal sensitive information.

To protect against QR code frauds and SIM swap frauds, it's important to be cautious when scanning QR codes, especially those found in public places or received through unsolicited messages. We should also be vigilant about protecting our personal information and passwords, and should regularly monitor our financial accounts and mobile phone activity for any suspicious activity.



CHECK YOUR PROGRESS

Q1. Choose the correct option:

(a) What is identity theft?

(i) A type of lottery scam

(ii) A type of investment scam

(iii) A type of email scam

(iv) A type of fraud where someone steals another person's personal information

(b) What is phishing?
   (i) A type of social engineering attack where fraudsters try to trick people into sharing their personal information or payment details
   (ii) A type of network attack
   (iii) A type of ransomware attack
   (iv) A type of malware attack

(c) What can be the consequences of identity theft?
   (i) Increased social media followers
   (ii) Greater financial stability
   (iii) Improved credit score
   (iv) Financial loss, damage to credit rating, and potential legal and criminal issues

(d) What is payment gateway fraud?

(i) Fraudulent activities that take place during the payment process

(ii) A type of phishing attack

(iii) A type of social engineering attack

(iv) A type of malware attack

(e) What are fake payment apps?
   (i) Legitimate mobile applications that are used for making payments
   (ii) Mobile applications that are used for social media
   (iii) Fraudulent mobile applications that masquerade as legitimate payment apps but are designed to steal users' personal and financial information
   (iv) Mobile applications that are used for online shopping for any suspicious activity.

(f) What is malware?
   (i) Malicious software programs that are designed to infiltrate and damage computer systems or mobile devices
   (ii) Software programs that are used for gaming
   (iii) Legitimate software programs that are used for productivity
   (iv) Software programs that are used for web browsing

(g) What are QR code frauds?
   (i) QR codes that are used for gaming
   (ii) Legitimate QR codes that are used for quick access to information
   (iii) The use of fraudulent QR codes that are designed to steal personal and financial information from unsuspecting victims
   (iv) QR codes that are used for social media

(h) What are SIM swap frauds?
   (i) A fraudulent transfer of a victim's mobile phone number to a new SIM card that is controlled by the fraudster
   (ii) A type of social engineering attack
   (iii) A type of phishing attack
   (iv) A type of network attack

(i) How can users protect against fake payment apps?
   (i) Use weak passwords
   (ii) Share personal and financial information with anyone who asks for it
   (iii) Download apps from untrusted sources
   (iv) Only download apps from trusted sources, such as official app stores

(j) How can users protect against SIM swap frauds?
   (i) Transfer mobile phone numbers to new SIM cards frequently
   (ii) Be cautious when sharing personal information and passwords
   (iii) Share personal information with anyone who asks for it
   (iv) Regularly monitor financial accounts and mobile phone activity for any suspicious activity

11.4 PREVENTIVE MEASURES FOR DIGITAL PAYMENT FRAUDS

11.4.1 Safe Browsing Practices and Password Management

Digital payment frauds can be prevented by following safe browsing practices and effective password management. Here are some tips on how to protect yourself:

(a) Use a strong password: A strong password should contain a combination of uppercase and lowercase letters, numbers, and symbols. We should avoid using common words or phrases as our password, as these can be easily guessed. We should also avoid using the same password for multiple accounts.

Here's an example of a strong password: b7K#nL@9$pDfTm2Z

This password includes uppercase and lowercase letters, numbers, and symbols. It is also long and complex, making it difficult for someone to guess or crack through brute-force attacks. It's important to note that a password like this would be difficult to remember, so using a password manager to securely store and generate unique passwords is recommended.

What is brute-force attack? It is a hacking method in which an attacker tries to guess a password or encryption key by systematically trying every possible combination of characters until the correct one is found. This is done using automated software that can quickly generate and test many different password combinations. Brute-force attacks can be effective against weak passwords that are short, common, or based on easily guessable information such as a person's name, birthdate, or simple dictionary words. However, strong passwords that are long and complex, using a combination of letters, numbers, and symbols, are much more resistant to brute-force attacks. Additionally, many online services and websites have built-in security measures to detect and prevent brute-force attacks, such as limiting the number of login attempts or requiring additional

forms of authentication such as two-factor authentication.

(b) Use a password manager: A password manager is a software tool that helps you create, store, and manage passwords for your various accounts. This makes it easy to use strong and unique passwords for each account without having to remember them all.

(c) Be wary of phishing scams: Phishing scams are fraudulent attempts to obtain sensitive information such as usernames, passwords, and credit card details by posing as a trustworthy entity in electronic communication. Here are some examples of phishing scams:

- **Email scams:** These are the most common types of phishing scams. Attackers send emails that appear to be from reputable sources, such as banks, online retailers, or social media platforms, asking users to click on a link or download an attachment. The link or attachment may contain malware that steals the user's information.
- **Fake websites:** Attackers create websites that look identical to legitimate websites, such as online shopping sites or banking portals. They use these fake websites to trick users into entering their login credentials, which the attackers then steal.
- **SMS scams:** Attackers send text messages to users claiming to be from legitimate sources, such as banks, asking for personal information or requesting that the user click on a link.
- **Spear phishing:** This type of phishing is more targeted and sophisticated. Attackers research their victims and send personalized emails that appear to be from a trusted source, such as a colleague or a boss. They may ask the victim to send money or share sensitive information.
- **Social media scams:** Attackers use social media platforms to send messages to users or create fake accounts to post links or messages. These messages may ask for personal information or direct users to fake websites.

It's important to be vigilant and to never share personal information

unless we are absolutely certain we are dealing with a legitimate source.

(d) Use a secure browser: Using a secure browser can help protect our online activities and personal information from unauthorized access. Here's a step-by-step guide on how to use a secure browser:

- **Choose a secure browser:** We need to look for a browser that has advanced security features, such as encryption, anti-phishing protection, and privacy settings. Popular secure browsers include Google Chrome, Mozilla Firefox, Apple Safari, and Microsoft Edge.
- **Keep our browser up to date:** We need to make sure we are using the latest version of our chosen browser. This will ensure that we have access to the latest security updates and features.
- **Install browser extensions:** We need to install browser extensions that enhance our security and privacy, such as an ad blocker, a password manager, and a VPN (virtual private network).
- **Configure our privacy settings:** We need to configure our browser's privacy settings to block third-party cookies, disable location tracking, and enable "Do Not Track" requests.
- **Avoid risky websites:** We need to avoid visiting risky websites, such as those that are known for distributing malware, spam, or phishing scams.
- **Check for secure connections:** We need to look for the padlock icon in the address bar to ensure that the website we are visiting has a secure connection. The website's URL should start with "https://" instead of "http://".
- **Be cautious with downloads:** We should be cautious when downloading files or software from the internet. We need to scan them with our antivirus software before opening them.

By following these steps, we can use a secure browser to browse the internet safely and protect your personal information.

(e) Keep our software up to date: We need to keep our operating system and software up to date with the latest security patches

and updates. This will help protect our computer or mobile device from known security vulnerabilities.

By following these safe browsing practices and password management tips, we can help prevent digital payment frauds and keep your personal and financial information secure.

11.4.2 Two-Factor Authentication and Biometric Authentication

Two-factor authentication (2FA) is a security process in which a user provides two different forms of identification before being granted access to a system, website, or application. This adds an extra layer of security to the login process and helps protect against unauthorized access, even if a password is compromised.

One example of 2FA is using a mobile phone to verify a user's identity. After entering their username and password, the user is prompted to enter a code that is sent to their mobile phone via text message or through an authentication app. This code is unique and changes frequently, so even if someone else knows the user's password, they won't be able to access the account without also having the user's phone.

11.4.3 Avoiding Public Wi-Fi and Using Trusted Payment Gateways

Preventive measures for digital payment frauds include several steps that users can take to protect their personal and financial information when making online transactions. Two of these steps include avoiding public Wi-Fi and using trusted payment gateways.

Avoiding Public Wi-Fi: Public Wi-Fi networks are generally not secure, and cybercriminals can intercept the data transmitted over these networks, including login credentials and payment information. As a result, it's best to avoid using public Wi-Fi networks when making online payments or accessing sensitive information. If we must use public Wi-Fi, it's important to use a virtual private network (VPN) to encrypt our data.

Using Trusted Payment Gateways: Trusted payment gateways are secure platforms that facilitate online payments. They offer additional security measures such as encryption and two-factor authentication to prevent fraudulent transactions. When making online payments, always use trusted payment gateways that are reputable and have good reviews. We should look for payment gateways that have been certified by payment card networks, such as Visa or Mastercard, to ensure they meet industry security standards.

11.4.4 Regularly Checking Transaction History and Setting Transaction Alerts

Preventive measures for digital payment frauds involve various actions that individuals can take to minimize the risk of fraud when making online transactions. One such measure is regularly checking transaction history, which involves reviewing all transactions made through digital payment channels to ensure that they are legitimate and authorized. This can help identify any suspicious activity and enable quick action to be taken to prevent further fraud.

Another measure is setting transaction alerts, which involves setting up notifications that alert individuals when a transaction is made using their digital payment account. This can help to identify fraudulent activity in real-time and enable quick action to be taken to prevent further fraud.



CHECK YOUR PROGRESS

Q2. Write short answers for the following questions:

(a) What is a strong password?

(b) What is a password manager?

(c) What are some examples of phishing scams?

(d) What is two-factor authentication?

(e) How can you use a secure browser?

11.5 RBI GUIDELINES ON DIGITAL PAYMENTS

11.5.1 Overview of RBI's Role in Regulating Digital Payments

The Reserve Bank of India (RBI) plays a crucial role in regulating digital payments in India. As the country's central bank, the RBI is responsible for ensuring the stability and efficiency of the payment system and for promoting financial inclusion.

Some of the key roles and responsibilities of the RBI in regulating digital payments include:

- **Issuing guidelines and regulations:** The RBI issues guidelines and regulations for digital payment service providers (PSPs) to ensure that they comply with the regulatory framework and operate in a safe and secure manner.
- **Oversight and supervision:** The RBI provides oversight and supervision of digital payment systems and services to ensure their safety, security, and reliability.
- **Licensing and authorization:** The RBI is responsible for licensing and authorizing payment system operators (PSOs) and payment intermediaries (PIs) to operate in India.
- **Consumer protection:** The RBI plays an important role in protecting the interests of consumers by setting standards for transparency, security, and efficiency in digital payments.
- **Innovation and development:** The RBI promotes innovation and development in digital payments by encouraging the adoption of new technologies and facilitating collaborations between PSPs, PSOs, and PIs.

Overall, the RBI's role in regulating digital payments is critical to ensure the safety, security, and efficiency of the payment system and to promote financial inclusion in India.

11.5.2 RBI Guidelines on Customer Protection in Digital Transactions

The Reserve Bank of India (RBI) has issued several guidelines on customer protection in digital transactions to ensure the safety and security of transactions carried out through digital channels. Some of these guidelines are:

- **Customer Consent:** Banks and other payment service providers must ensure that customers give their explicit consent for any digital transaction.
- **Two-factor Authentication:** All digital transactions must have a two-factor authentication system in place, which requires customers to enter a unique password or OTP sent to their registered mobile number or email address.
- **Customer Education:** Banks and payment service providers must educate their customers about the risks and best practices of using digital channels for transactions.
- **Complaint Redressal:** Banks and payment service providers must have a proper complaint redressal mechanism in place to handle customer complaints related to digital transactions.
- **Security Measures:** Banks and payment service providers must have robust security measures in place to protect customers' personal and financial information from cyber-attacks.
- **Limits on Transactions:** Banks and payment service providers must set limits on the amount of money that can be transacted through digital channels to prevent large-scale fraud.
- **Reporting:** Banks and payment service providers must report any fraud or unauthorized transactions to the RBI within a specified time frame.

These guidelines aim to protect customers from fraud and unauthorized transactions in the digital world and encourage the adoption of digital transactions in a safe and secure manner.

11.5.3 Complaint Redressal Mechanisms and Dispute Resolution Procedures

The RBI guidelines on digital payments mandate that banks and payment service providers must have proper complaint redressal mechanisms and dispute resolution procedures in place to address any grievances or disputes related to digital transactions. Here are some of the key aspects of these mechanisms and procedures:

- **Grievance Redressal Officer:** Banks and payment service providers must appoint a Grievance Redressal Officer to handle customer complaints related to digital transactions.
- **Timelines for Resolution:** The RBI guidelines specify timelines for the resolution of complaints and disputes related to digital payments. For example, banks must acknowledge complaints within three working days and resolve them within 30 days.
- **Escalation Matrix:** Banks and payment service providers must have an escalation matrix in place for cases where complaints are not resolved within the specified time frame. Customers can escalate their complaints to higher authorities within the organization or to the RBI.
- **Complaint Registration:** Banks and payment service providers must provide multiple channels for customers to register their complaints, such as phone, email, or online forms.
- **Dispute Resolution Mechanisms:** Banks and payment service providers must have a dispute resolution mechanism in place for cases where there is a dispute between the customer and the merchant or payment service provider. The RBI has also introduced a dispute resolution scheme for digital transactions, which is mandatory for all payment system operators.

Overall, the complaint redressal mechanisms and dispute resolution procedures mandated by the RBI guidelines aim to ensure that customers have a recourse for any grievances or disputes related to digital transactions and that their interests are protected.

11.6 PAYMENT SETTLEMENT ACT, 2007

11.6.1 Overview of the Payment Settlement Act, 2007

The Payment and Settlement Systems Act, 2007 is an Indian legislation that provides for the regulation and supervision of payment and settlement systems in the country. The Act was passed by the Indian Parliament in December 2007 and came into effect from August 2008. The main objectives of the Act are to:

- Promote the development and regulation of payment and settlement systems in India.
- Ensure the stability and efficiency of payment and settlement systems in the country.
- Protect the interests of consumers in payment and settlement systems.
- Encourage the use of electronic modes of payment and settlement.

Some of the key provisions of the Payment and Settlement Systems Act, 2007 are:

- **Regulation of Payment and Settlement Systems:** The Act provides for the regulation and supervision of payment and settlement systems by the Reserve Bank of India (RBI).
- **Authorization of Payment System Operators:** The Act requires all payment system operators to be authorized by the RBI before they can commence operations.
- **Settlement Finality:** The Act provides for settlement finality, which means that once a transaction is settled, it cannot be reversed.
- **Netting:** The Act allows for netting of payments, which means that payments can be offset against each other to reduce settlement risks.
- **Consumer Protection:** The Act mandates payment system operators to ensure the security and confidentiality of customer

data, and to have a complaint redressal mechanism in place for customer grievances.

- **Powers of RBI:** The Act empowers the RBI to issue directions, regulate fees and charges, and inspect payment system operators.

Overall, the Payment and Settlement Systems Act, 2007 provides a legal framework for the regulation and supervision of payment and settlement systems in India, with a focus on promoting efficiency, stability, and consumer protection in the payments ecosystem.

11.6.2 Provisions Related to Payment Systems, Payment Gateways, and Payment Settlement

The Payment and Settlement Systems Act, 2007 provides for the regulation and supervision of payment systems, payment gateways, and payment settlement in India. Here are some of the key provisions related to these areas:

- **Payment Systems:** The Act defines payment systems as any system that enables payment transactions between a payer and a beneficiary, and includes systems for processing credit card transactions, electronic funds transfer, and mobile payments. The Act provides for the regulation and supervision of payment systems by the Reserve Bank of India (RBI).
- **Payment Gateways:** The Act defines payment gateways as entities that provide technology infrastructure to route and process payment transactions between a merchant and a customer. Payment gateways must be authorized by the RBI before they can commence operations. The Act also mandates payment gateways to ensure the security and confidentiality of customer data.
- **Payment Settlement:** The Act provides for settlement finality, which means that once a payment transaction is settled, it cannot be reversed. The Act allows for netting of payments, which means

that payments can be offset against each other to reduce settlement risks. The Act also provides for the establishment of a Payment and Settlement Systems Fund, which can be used to mitigate settlement risks in the payments ecosystem.

- **Authorization of Payment System Operators:** The Act requires all payment system operators to be authorized by the RBI before they can commence operations. The Act empowers the RBI to issue directions to payment system operators, regulate fees and charges, and inspect their operations.
- **Consumer Protection:** The Act mandates payment system operators and payment gateways to ensure the security and confidentiality of customer data, and to have a complaint redressal mechanism in place for customer grievances. The Act also provides for the imposition of penalties and fines for non-compliance with its provisions.

Overall, the Payment and Settlement Systems Act, 2007 provides a legal framework for the regulation and supervision of payment systems, payment gateways, and payment settlement in India, with a focus on promoting efficiency, stability, and consumer protection in the payments ecosystem.

11.6.3 Legal Implications of Unauthorized Transactions and Payment Frauds Under the Act

The Payment and Settlement Systems Act, 2007 provides for legal implications in case of unauthorized transactions and payment frauds. Here are some of the key provisions related to these areas:

- **Unauthorized Transactions:** The Act mandates payment system operators and payment gateways to put in place adequate security measures to prevent unauthorized transactions. If an unauthorized transaction takes place, the Act provides for liability of the payment system operator, payment gateway, and the customer, depending on the circumstances of the transaction. If

the customer has notified the payment system operator of the unauthorized transaction within a reasonable time, the liability of the customer is limited to a certain amount as specified by the RBI. If the customer has not notified the payment system operator within a reasonable time, the liability of the customer can be unlimited.

- **Payment Frauds:** The Act provides for penalties and fines for payment frauds. Any person who commits a payment fraud can be punished with imprisonment for up to three years, or with a fine of up to five lakh rupees, or both. The Act also provides for the imposition of penalties on payment system operators and payment gateways that fail to comply with its provisions, including those related to preventing payment frauds.
- **Consumer Protection:** The Act mandates payment system operators and payment gateways to have a complaint redressal mechanism in place for customer grievances related to unauthorized transactions and payment frauds. Customers can approach the ombudsman appointed by the RBI for resolution of their complaints. The Act also empowers the RBI to impose penalties and fines on payment system operators and payment gateways that fail to protect the interests of consumers.

Overall, the Payment and Settlement Systems Act, 2007 provides a legal framework for dealing with unauthorized transactions and payment frauds, with a focus on protecting the interests of consumers and ensuring the stability and efficiency of payment systems in India.



CHECK YOUR PROGRESS

Q3. Choose the correct option:

(a) What is the main objective of the Payment and Settlement Systems Act, 2007?

(A) To promote the development and regulation of payment and settlement systems in India.

(B) To protect the interests of consumers in payment and settlement systems.

(C) To encourage the use of electronic modes of payment and settlement.

(D) All of the above.

(b) What is the role of the RBI in regulating digital payments in India?

(A) Issuing guidelines and regulations.

(B) Oversight and supervision.

(C) Licensing and authorization.

(D) All of the above.

(c) What is the two-factor authentication system mandated by the RBI guidelines on customer protection in digital transactions?

(A) Customers must enter a unique password or OTP sent to their registered mobile number or email address.

(B) Customers must provide their name and address for every transaction.

(C) Customers must provide their bank account number and IFSC code for every transaction.

(D) Customers must provide their Aadhaar number for every transaction.

(d) What is the role of the Grievance Redressal Officer in the complaint redressal mechanism mandated by the RBI guidelines on digital payments?

(A) To appoint the customer to a higher authority within the organization.

(B) To provide multiple channels for customers to register their complaints.

(C) To handle customer complaints related to digital transactions.

(D) To provide a dispute resolution mechanism for cases of dispute between the customer and the merchant or payment service provider.

(e) What is the dispute resolution scheme introduced by the RBI for digital transactions?

(A) A system for netting of payments to reduce settlement risks.

(B) A mechanism for reporting fraud or unauthorized transactions to the RBI.

(C) A mandatory dispute resolution mechanism for all payment system operators.

(D) A security measure to protect customers' personal and financial information from cyber-attacks.



11.7 LET US SUM UP

- Common frauds in digital payments include identity theft, phishing scams, unauthorized transactions, payment gateway frauds, fake payment apps, malware attacks, QR code frauds, and SIM swap frauds.
- These frauds can result in financial losses, damage to credit scores, and identity theft.
- To prevent these frauds, users should keep their payment information secure, use reputable payment processors, only download apps from trusted sources, and regularly monitor their financial accounts for suspicious activity.
- Users should also be cautious when clicking on links or downloading attachments from unknown sources, and should be vigilant about protecting their personal information and passwords.
- To prevent digital payment frauds, users should follow safe browsing practices and effective password management, such as using strong passwords and a password manager.
- Users should also be wary of phishing scams, which are fraudulent attempts to obtain sensitive information, and should use a secure browser and keep their software up to date.
- Two-factor authentication and biometric authentication can add an extra layer of security to the login process and help protect against unauthorized access.

- Financial institutions should also implement fraud detection and prevention systems to detect and prevent fraudulent transactions.
- The Payment and Settlement Systems Act, 2007 is an Indian legislation that regulates and supervises payment and settlement systems in the country.
- The Act provides for the authorization of payment system operators, settlement finality, netting of payments, and consumer protection.
- The Act defines payment systems, payment gateways, and payment settlement, and mandates payment gateways to ensure the security and confidentiality of customer data.
- The Act provides for legal implications in case of unauthorized transactions and payment frauds, including penalties, fines, and liability for payment system operators, payment gateways, and customers.



11.8 ANSWER TO CHECK YOUR PROGRESS

Ans.to. Q. No.1:

(a) (iv)	(b) (i)	(c) (iv)	(d) (i)	(e) (iii)
(f) (i)	(g) (iii)	(h) (i)	(i) (iv)	(j) (iv)

Ans.to Q.No.2(a): A strong password should contain a combination of uppercase and lowercase letters, numbers, and symbols.

Ans.to Q.No.2(b): A password manager is a software tool that helps you create, store, and manage passwords for your various accounts.

Ans.to Q.No.2(c): Email scams, fake websites, SMS scams, spear phishing, and social media scams are some examples of phishing scams.

Ans.to Q.No.2(d): Two-factor authentication (2FA) is a security process in which a user provides two different forms of identification before being granted access to a system, website, or application.

Ans.to Q.No.2(e): You can use a secure browser by choosing a browser that has advanced security features, keeping your browser up to date, installing browser extensions, configuring your privacy settings, avoiding risky websites, checking for secure connections, and being cautious with downloads.

Ans.to Q.No.3: (a) (D) (b) (D) (c) (A) (d) (C) (e)(C)



11.9 FURTHER READINGS

1) Cyber Crime Impact in the New Millennium, by R. C Mishra ,AutherPress. Edition 2010.
2) Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by SumitBelapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)
3) Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
4) Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
5) Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
6) Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
7) Fundamentals of Network Security by E. Maiwald, McGraw Hill.



11.10 MODEL QUESTIONS

Q.1: What are some common types of payment gateway frauds, and how can they be prevented?

Q.2: What are some best practices for protecting against identity theft and phishing scams in digital payments?

Q.3: How do fake payment apps work, and what are some ways to protect against them?

Q.4: What are some dangers of QR code frauds and SIM swap frauds, and how can users protect themselves against these types of fraud?

Q.5: What are some key steps that victims of unauthorized transactions or payment gateway frauds should take to protect their accounts and prevent further losses?

Q.6: What is a strong password, and why is it important to have one?

Q.7: What is a password manager, and how can it help prevent digital payment fraud?

Q.8: What are some common types of phishing scams, and how can you avoid them?

Q.9: What is two-factor authentication, and how does it add an extra layer of security to the login process?

Q.10: What are some safe browsing practices, and how can they help protect against digital payment fraud?

Q.11: What is the role of the Reserve Bank of India (RBI) in regulating digital payments?

Q.12: What are some of the guidelines issued by the RBI to protect customers in digital transactions?

Q.13: What are the complaint redressal mechanisms and dispute resolution procedures mandated by the RBI guidelines?

Q.14: What are the key objectives of the Payment and Settlement Systems Act, 2007 in India?

Q.15: What are some of the provisions of the Payment and Settlement Systems Act, 2007 related to the regulation of payment and settlement systems in India?

*** ***** ***

UNIT 12: DIGITAL DEVICE SECURITY I

UNIT STRUCTURE

12.1 Learning Objectives

12.2 Introduction

12.3 End Point Device and Mobile Phone Security

12.4 Password Policy

12.5 Security Patch Panagement

12.6 Data Backup

12.7 Downloading and Management of Third Party Software

12.8 Let Us Sum Up

12.9 Answers To Check Your Progress

12.10 Further Readings

12.11 Model Questions

12.1 LEARNING OBJECTIVES

After going through this unit, you will be able to :

- understand the basic concepts of Digital Device Security
- understand the device security policy and password policy
- assist in fixing code bugs or bugs in system applications
- download and manage third party software

12.2 INTRODUCTION

In this unit, we are going to learn about basic concepts of digital device security. Digital device security refers to the protection of digital information and technology assets from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves a range of measures designed to ensure the confidentiality, integrity, and availability of data and systems.Digital device security encompasses various areas, such as network security, information security, application security, and device security. It involves the use of encryption, firewalls, antivirus software, access

controls, and other tools and techniques to protect digital assets from cyber threats, such as malware, phishing attacks, hacking, and identity theft.Digital device security is essential in today's world, where technology is increasingly integrated into every aspect of our lives, and sensitive information is stored and transmitted electronically. Effective digital device security practices can help prevent data breaches, protect personal privacy, and safeguard critical infrastructure and national security.In this chapter, we are also going to discuss the how we can protect an organization's network and data from potential security threats by securing the different endpoints devices.We are also going to look at device security policy, security patch management, the concept of data backup and some best practices for downloading and managing third-party software.

12.3 END POINT DEVICE AND MOBILE PHONE SECURITY

Endpoint devices, also known as end-user devices, refer to any device that serves as an endpoint in a network, meaning it is the final destination of data packets sent over the network. Some common examples of endpoint devices include:

- Desktop computers
- Laptops
- Tablets
- Smartphones
- Printers
- Scanners
- Copiers
- Fax machines
- IP phones
- VoIP phones
- POS (Point of Sale) systems
- Medical devices
- Industrial control systems
- Smart home devices, such as smart thermostats and security systems

- Internet of Things (IoT) devices, such as smart watches and fitness trackers etc.

Endpoint devices are often the most vulnerable point of entry for cyber threats, as they are typically used by employees to access critical business information, and can be easily targeted by hackers seeking to gain access to the network. This has led to the development of endpoint security solutions, which are designed to protect these devices from malware, viruses, and other cyber threats. Endpoint security solutions typically include antivirus software, firewalls, intrusion detection systems, and endpoint management tools, which can be used to monitor and manage the security of endpoint devices across a network. They may also include features such as data encryption, secure remote access, and access controls to prevent unauthorized access to sensitive information.

As more organizations adopt remote work policies and mobile devices become increasingly prevalent, endpoint security has become a critical component of overall cyber security strategy. Effective endpoint security requires a multi-layered approach, including both technology solutions and employee training and awareness programs, to ensure that endpoint devices are secure and protected from cyber threats.

Endpoint security is the protection of an organization's network and data from potential security threats by securing the endpoints, such as laptops, desktops, mobile devices, and other smart devices. Endpoint device security architecture is the design of a comprehensive security solution that includes various security measures to protect endpoints from potential security threats. The endpoint security architecture includes various layers of security measures that work together to protect the endpoints from potential security threats. These measures include:

- **Endpoint protection platform (EPP):** EPP is a security solution that protects endpoints from malware, viruses, and other malicious software. EPP includes features such as antivirus, firewalls, intrusion detection, and prevention systems.
- **Endpoint detection and response (EDR):** EDR is a security solution that provides real-time threat detection and response to

potential security threats. EDR includes features such as endpoint behavioral analysis, threat hunting, and incident response.

- **Patch management:** Patch management is the process of updating the software and applications on endpoints with the latest security patches and updates. Patch management helps to ensure that endpoints are protected from known vulnerabilities.
- **Mobile device management (MDM):** MDM is a security solution that manages and secures mobile devices, such as smartphones and tablets. MDM includes features such as device encryption, remote wipe, and application whitelisting.
- **Data loss prevention (DLP):** DLP is a security solution that prevents sensitive data from leaving the organization's network. DLP includes features such as content filtering, data classification, and data encryption.
- **Identity and access management (IAM):** IAM is a security solution that manages user identities and access to endpoints and data. IAM includes features such as multi-factor authentication, password management, and role-based access control.

Endpoint device security architecture should be designed based on the organization's security policies and risk management strategies. The architecture should be flexible and scalable to accommodate the organization's changing security needs. Additionally, the architecture should be regularly updated and tested to ensure that it is effective against potential security threats.

Endpoint device security architecture is critical in protecting an organization's network and data from potential security threats. The architecture includes various layers of security measures, such as EPP, EDR, patch management, MDM, DLP, and IAM, that work together to provide a comprehensive security solution for endpoints. A well-designed endpoint device security architecture can help to minimize security risks and protect the organization's valuable assets.

Mobile Phone Security :

On the other hand, the mobile security or mobile device security is the protection of smartphones, tablets, and laptops against wireless computing threats. This is becoming increasingly important in mobile computing. The security of personal and business information stored on smartphones is a particular concern these days.

Most of the users and companies are using smartphones not only to communicate, but also to plan and organize their work and private life. Within companies, these technologies cause profound changes in the organization of information systems and thus become a source of new risks. Indeed, smartphones collect and compile increasingly sensitive information, access to which must be controlled to protect the privacy of users and the intellectual property of companies. Most attacks target smartphones. These attacks exploit vulnerabilities present in smartphones that can be generated by different communication methods, including short message service (SMS), multimedia messaging service (MMS), wireless, Bluetooth and GSM connections, which are of de facto the international standard. Code division multiple access (CDMA) is more secure than other communication methods, but can still be a target. Another weakness is the operating system or browser of the smartphone. Some malware exploits the limited knowledge of ordinary users. According to a 2008 McAfee study, only 2.1% of users said they had been directly exposed to mobile malware, which revealed that 11.6% had heard of other people affected by the problem. However, this number is expected to increase.Security measures are developed and applied to smartphones, from security best practices for software to the distribution of information to end users. Countermeasures can be implemented at different levels, including operating system development, software design, and user behavior modification.

Challenges of smartphone mobile security:

- **Malware attacks:** Malware is malicious software that can infect smartphones through downloaded apps, phishing links, or insecure network connections. Malware can steal personal data, monitor activities, and even hijack the device's functionality.

- **Data breaches:** Smartphones often store sensitive personal data, such as banking information, social security numbers, and passwords. Data breaches can occur when this data is accessed by unauthorized users, either through hacking or social engineering.
- **Insecure wireless connections:** Public Wi-Fi networks, such as those found in cafes, airports, and hotels, can be vulnerable to hackers who use them to intercept and steal data transmitted over the network.
- **Device loss or theft:** Losing a smartphone or having it stolen can be a major security risk, as it can provide unauthorized access to the device's data and functionality.
- **Operating system vulnerabilities:** Like any software, mobile operating systems have their own vulnerabilities that can be exploited by cybercriminals to gain access to sensitive data or control of the device.
- **Insecure applications:** Third-party apps downloaded from unofficial sources or with inadequate security measures can provide an easy entry point for hackers into a smartphone.
- **Social engineering attacks:** Cybercriminals can use social engineering tactics such as phishing emails, text messages, or phone calls to trick smartphone users into revealing sensitive information or installing malicious software.

When a smartphone is infected by an attacker, the attacker can attempt a variety of malicious actions depending on their objectives. Here are some of the most common actions that an attacker can take:

- **Steal sensitive data:** The attacker can steal sensitive personal data, such as login credentials, financial information, contacts, and messages.
- **Monitor activities:** The attacker can monitor the user's activities, such as recording keystrokes or capturing screenshots, to collect sensitive information or gain access to accounts.
- **Hijack functionality:** The attacker can take control of the smartphone's functionality, such as making calls, sending text

messages, or accessing the camera and microphone.

- **Send premium text messages:** The attacker can use the smartphone to send premium text messages to a premium rate number, resulting in high charges for the user.
- **Spread malware:** The attacker can use the infected smartphone to spread malware to other devices in the network, either by sending infected files or through the smartphone's Bluetooth or Wi-Fi connectivity.
- **Use the device as part of a botnet:** The attacker can use the infected smartphone as part of a botnet, a network of compromised devices used to carry out distributed denial-of-service (DDoS) attacks or other cyber attacks.
- **Ransomware:** The attacker can encrypt the user's data and demand a ransom payment in exchange for the decryption key.

Let us look into few more attacks :

Attacks based on communication

Attack based on SMS and MMS: Attackers can use SMS and MMS to carry out various types of attacks on smartphones. These attacks include smishing, a form of phishing attack that uses SMS to trick users into revealing sensitive information or downloading malware. Attackers can also send MMS messages with malicious links or attachments that, when opened, can download malware onto the user's smartphone. Another common attack is premium rate SMS fraud, where attackers send SMS messages to premium rate numbers that charge high fees, resulting in financial losses for the user. Additionally, attackers can flood a smartphone with a large number of SMS or MMS messages, causing the device to crash or become unresponsive.

Attacks based on communication networks

Attacks based on the GSM networks:GSM (Global System for Mobile Communications) networks, which are used by most mobile carriers around the world, are also vulnerable to various types of attacks. One common attack is known as the "man-in-the-middle" attack, where an attacker intercepts the

communication between a mobile device and the GSM network to eavesdrop on calls or steal sensitive information. Another attack is the “fake base station” attack, where an attacker sets up a fake GSM base station to intercept mobile devices’ communication and gain access to sensitive information. Attackers can also perform “IMSI-catcher” attacks, where they use a device that masquerades as a legitimate GSM tower and forces mobile devices to connect to it, allowing the attacker to intercept calls and text messages.

Attacks based on Wi-Fi:

Attackers can try to eavesdrop on Wi-Fi communications for information (eg usernames, passwords). This type of attack is not unique to smartphones, but they are vulnerable to it because Wi-Fi is often the only means of communication and they need to have access to the Internet. Therefore, the security of wireless networks (WLAN) is an important topic. Initially, wireless networks are protected by WEP keys.The weakness of WEP is that all connected clients use the same short encryption key. Additionally, the researchers found a reduction in the key search space. Today, most wireless networks are protected by the WPA security protocol. WPA is based on the Temporal Key Integrity Protocol (TKIP) and was designed to allow migration from WEP to WPA on deployed devices. The most significant security enhancement is to dynamic encryption keys.

For small networks, WPA is based on a shared key called a “pre-shared key”. If the shared key length is short, the cipher can be attacked. With limited input possibilities (i.e. only numeric keypad), mobile phone users can define short encryption keys that only contain numbers. There are many risks associated with their unsecured Wi-Fi networks. One common attack is the “rogue access point” attack, where an attacker sets up a fake Wi-Fi hotspot that appears to be legitimate, but actually intercepts traffic and steals sensitive information. Another attack is the “man-in-the-middle” attack, where an attacker intercepts traffic between a mobile device and a Wi-Fi network to eavesdrop on communication or steal sensitive information. Attackers can also use “packet sniffing” to capture and analyze network traffic, allowing them to steal login credentials or other sensitive information.

Bluetooth-based attacks

Bluetooth technology, which is commonly used for wireless communication between devices, is also vulnerable to various types of attacks. One principle of Bluetooth-based attacks is that an attacker can exploit vulnerabilities in the Bluetooth protocol or in specific Bluetooth devices to gain unauthorized access to a device or its data. For example, an attacker can use “bluejacking” to send unsolicited messages or files to nearby Bluetooth-enabled devices, potentially causing the devices to crash or perform unintended actions. Another attack is “bluesnarfing,” where an attacker can gain unauthorized access to a device’s data, such as contact lists, text messages, or emails, by exploiting vulnerabilities in the Bluetooth protocol. Attackers can also use “bluebugging” to take over a Bluetooth-enabled device, allowing them to make calls, send messages, or access data on the device without the user’s knowledge or consent.

Attacks based on vulnerabilities in software applications:

One of the most common ways attackers can target mobile devices is by exploiting vulnerabilities in software applications. Attackers can use various techniques to exploit vulnerabilities in software applications on mobile devices, such as malware injection, data leakage, and buffer overflow attacks. Malware injection involves exploiting vulnerabilities in an application to inject malicious code that can steal sensitive information, modify the behavior of the application, or control the device. For example, attackers can use this technique to create a fake login screen in a legitimate banking application and steal the user’s login credentials. Data leakage attacks involve gaining unauthorized access to sensitive data stored within an application, such as login credentials or financial information. For example, attackers can use this technique to steal personal information stored in a health application.

Buffer overflow attacks involve exploiting vulnerabilities in an application’s memory management and executing arbitrary code on the device. This technique can be used to take control of a device, steal sensitive data, or modify the behavior of an application. For example, attackers can use this technique to execute malicious code in a browser application and steal sensitive information.

Attacks based on hardware vulnerabilities:

Hardware vulnerabilities can be exploited by attackers to manipulate the hardware components of a device, bypass security measures, or install malicious software. One example of a hardware-based attack on mobile devices is known as a “side-channel attack.” In a side-channel attack, attackers use the physical characteristics of a device’s hardware, such as power consumption or electromagnetic emissions, to gain access to sensitive information. This type of attack can be used to steal cryptographic keys, passwords, or other sensitive information.

Another example of a hardware-based attack is known as a “chip-level attack.” In a chip-level attack, attackers manipulate the hardware components of a device to bypass security measures or gain control of the device. For example, attackers can use this technique to extract encryption keys, install malware, or modify the behavior of the device.

Mobile malware:

Since smartphones are permanent access points to the internet (mostly online), they can be compromised just as easily as computers with malware. Malware is a computer program designed to damage the system on which it is installed. Trojans, worms, and viruses are all considered malware. A Trojan horse is a program on a smartphone that allows outside users to connect secretly.A worm is a program that replicates on multiple computers over a network. A virus is malicious software designed to spread to other computers by inserting itself into a legitimate program and running the program alongside it. However, it is clear that malware is much less numerous and less important on smartphones than on computers.

Countermeasures for mobile device security:

There are several countermeasures that can be taken to improve mobile device security and protect against various security threats. Here are some common countermeasures:

- **Use strong passwords and/or biometric authentication:** This can prevent unauthorized access to the device and the data it contains.
- **Keep the device up-to-date:** Regularly update the operating system and applications on the device to ensure that any known vulnerabilities are patched.
- **Install and use security software:** Install reputable antivirus and anti-malware software to scan for and remove threats from the device.
- **Use encryption:** Encryption can protect sensitive data on the device and during data transmission, preventing unauthorized access.
- **Avoid public Wi-Fi networks:** Public Wi-Fi networks can be insecure and can expose the device to security threats. Use a Virtual Private Network (VPN) when using public Wi-Fi.
- **Be cautious with downloads and app installations:** Only download apps from trusted sources, and be wary of apps that request access to sensitive data or system resources.
- **Enable remote wipe and backup:** In case the device is lost or stolen, remote wipe can erase all data on the device, and backup can ensure that data is not lost.
- **Use device management solutions:** Organizations can use mobile device management (MDM) solutions to enforce security policies and remotely manage and monitor devices.

By implementing these countermeasures, users can improve mobile device security and reduce the risk of security threats. However, it's important to note that no security measure is foolproof, and users should stay vigilant and informed about the latest security threats and best practices.

12.4 PASSWORD POLICY

A password policy is a set of rules and requirements that dictate how passwords should be created, stored, and managed in an organization or system. The purpose of a password policy is to enhance the security of the

system by ensuring that passwords are strong, unique, and protected from unauthorized access.

Here are some common elements that may be included in a password policy:

- **Password length:** The policy may specify a minimum and maximum length for passwords, typically ranging from 8 to 16 characters.
- **Complexity requirements:** The policy may require that passwords contain a mix of uppercase and lowercase letters, numbers, and special characters.
- **Password expiration:** The policy may require users to change their passwords periodically, such as every 90 days, to reduce the risk of password compromise.
- **Password history:** The policy may prevent users from reusing their previous passwords, to prevent attackers from guessing a reused password.
- **Account lockout:** The policy may automatically lock out an account after a certain number of failed login attempts to prevent brute-force attacks.
- **Two-factor authentication:** The policy may require users to use an additional factor, such as a mobile phone, to verify their identity when logging in.
- **Password storage:** The policy may require passwords to be stored securely, such as by hashing and salting, to protect them from unauthorized access.

By implementing a strong password policy, organizations can reduce the risk of security breaches caused by weak or compromised passwords.

12.5 SECURITY PATCH MANAGEMENT

Security patch management refers to the process of identifying, prioritizing, testing, deploying, and verifying software patches and updates to protect computer systems and networks from known vulnerabilities and

exploits. Patch management is an essential aspect of cybersecurity that helps organizations to ensure the security and reliability of their systems and networks.Cybersecurity threats are becoming increasingly sophisticated, and cybercriminals are continuously discovering new vulnerabilities and exploits to exploit. To stay ahead of these threats, it is crucial for organizations to regularly update their software and systems with the latest security patches and updates.Failing to update software and systems can leave organizations vulnerable to cyber attacks such as malware, ransomware, and phishing attacks, which can lead to data breaches, financial losses, and reputational damage.Security patch management helps organizations to mitigate these risks by ensuring that software vulnerabilities are identified and patched promptly. By doing so, organizations can reduce the window of opportunity for cybercriminals to exploit these vulnerabilities, thereby minimizing the risk of a successful cyber attack.

The Security Patch Management Process: The security patch management process involves several steps, including:

- **Identification -** This step involves identifying software vulnerabilities and patches that need to be applied. This can be done through various means, including vulnerability scans, security bulletins, and notifications from vendors.
- **Prioritization -** Once vulnerabilities are identified, they need to be prioritized based on their severity and the potential impact on the organization. This helps to ensure that patches are applied in a timely manner to mitigate the most significant risks.
- **Testing -** Before applying patches, they should be tested in a non-production environment to ensure that they do not cause any adverse effects on the system or application. This step is essential to prevent any downtime or disruption to critical business operations.
- **Deployment -** Once patches have been tested and verified, they can be deployed to the production environment. This can be done manually or through automated patch management tools.

- **Verification -** After patches have been deployed, it is essential to verify that they have been applied correctly and that the system or application is functioning correctly.

Challenges of Security Patch Management: Despite the importance of security patch management, many organizations face significant challenges when implementing it. Some of the most common challenges include:

- **Complexity -** The patch management process can be complex, particularly for large organizations with multiple systems and applications. This complexity can make it challenging to identify vulnerabilities and deploy patches effectively.
- **Prioritization -** Prioritizing patches can be challenging, particularly when dealing with a large number of vulnerabilities. Organizations need to balance the severity of the vulnerability with the potential impact on the organization.
- **Testing -** Testing patches can be time-consuming and resource-intensive, particularly for complex systems and applications. This can result in delays in patch deployment, leaving organizations vulnerable to cyber attacks.
- **Compliance -** Many organizations need to comply with regulatory requirements, which can add an additional layer of complexity to the patch management process. Failure to comply with these requirements can result in significant financial penalties and reputational damage.
- **Patching third-party software -** Many organizations use third-party software that may not be supported by the software vendor. This can make it challenging to identify and patch vulnerabilities in these applications, leaving organizations vulnerable to cyber attacks.

Best Practices for Security Patch Management: However, patch management can be a complex process, and many organizations struggle to implement an effective patch management strategy. We next discuss best practices for security patch management.

- **Establish a Patch Management Policy:** Organizations should develop a formal patch management policy that outlines the patch management process, roles and responsibilities, and timelines for patch deployment. The policy should also include guidelines on how to handle critical patches, such as those that address zero-day vulnerabilities. The policy should be communicated to all employees, and regular training sessions should be conducted to ensure everyone understands the policy.
- **Perform Regular Vulnerability Scans:** Regular vulnerability scanning should be conducted to identify vulnerabilities in systems and applications. Vulnerability scanning should be performed on a regular basis, such as monthly or quarterly, and after any significant changes to the infrastructure. Vulnerability scanning should be automated wherever possible to reduce the risk of human error and ensure consistency.
- **Prioritize Patches:** Patches should be prioritized based on their severity and the potential impact on the organization. Critical patches, such as those that address zero-day vulnerabilities or vulnerabilities that are actively being exploited, should be deployed as soon as possible. Non-critical patches should be prioritized based on their impact on business operations and the potential for exploitation.
- **Test Patches Before Deployment:** Patches should be tested thoroughly in a non-production environment before being deployed to the production environment. Testing should ensure that the patch does not cause any adverse effects on the system or application, such as crashes or performance issues. Testing should be automated wherever possible to reduce the risk of human error and ensure consistency.
- **Deploy Patches Quickly:** Patches should be deployed as quickly as possible after they are tested and verified. Delaying patch deployment increases the window of opportunity for hackers and cybercriminals to exploit vulnerabilities.

- **Automate Patch Management:** Automated patch management tools should be used wherever possible to streamline the patch management process and reduce the risk of human error. Automated tools can help with patch identification, prioritization, testing, and deployment.
- **Monitor and Verify Patch Deployment:** After patches are deployed, they should be monitored and verified to ensure they were applied correctly and that the system or application is functioning correctly. Monitoring can be done through vulnerability scanning, log analysis, or other security monitoring tools.
- **Conduct Regular Patch Audits:** Regular patch audits should be conducted to ensure that all systems and applications are up to date with the latest patches. Patch audits can help identify systems or applications that have not been patched or are not being patched in a timely manner.
- **Establish a Patch Rollback Plan:** In case a patch causes adverse effects on the system or application, a patch rollback plan should be established. The plan should outline the steps to revert the system or application to its previous state before the patch was deployed.
- **Compliance with Regulations and Standards:** Organizations should ensure that their patch management process complies with regulatory requirements and industry standards. Compliance with regulations and standards helps ensure that the organization is protected from financial penalties and reputational damage.

Effective security patch management is critical to protecting an organization's systems and applications from cyber attacks. Implementing best practices such as establishing a patch management policy, performing regular vulnerability scans, prioritizing patches, testing patches before deployment, deploying patches quickly, automating patch management, monitoring and verifying patch deployment, conducting regular patch audits, establishing a patch rollback plan, and complying with regulations and standards can help organizations develop an effective patch management strategy.

12.6 DATA BACKUP

Data backup is an essential aspect of data management, ensuring that critical data is protected against loss, corruption, or unauthorized access. Backing up data involves creating a copy of data, either manually or through automated processes, and storing it in a secure location. In this unit, we will discuss data backup in detail, including its importance, types of backups, backup strategies, and best practices.Data backup is critical for various reasons, including:

Disaster Recovery: Data backup is an essential part of disaster recovery planning. In case of a disaster, such as a natural calamity or a cyberattack, data backup ensures that data can be recovered, minimizing the impact on the organization.

Data Loss Prevention: Data loss can occur due to various reasons, including hardware failure, software errors, and accidental deletion. Data backup ensures that critical data can be restored, minimizing the risk of data loss.

Compliance: Many industries have regulatory requirements that mandate data backup for a specific period. Compliance with these regulations is crucial for avoiding legal and financial penalties.

Cost Savings: Data loss can result in significant financial losses, including lost productivity, downtime, and recovery costs. Data backup helps minimize these costs by ensuring that data can be restored quickly and efficiently.

Types of Backups : Let us now look at the types of backups

There are various types of backups, including:

- **Full Backup:** A full backup involves copying all data on a system or device. Full backups take longer to perform and require more storage space but offer comprehensive data protection.
- **Incremental Backup:** Incremental backups copy only the data that has changed since the last backup, making them faster and requiring less storage space than full backups.

- **Differential Backup:** Differential backups copy all the data that has changed since the last full backup, making them faster than full backups but slower than incremental backups.
- **Mirror Backup:** A mirror backup involves creating an exact copy of the data on a system or device, making it useful for disaster recovery.

Backup Strategies: Organizations can use various backup strategies, depending on their needs and resources. Some common backup strategies include:

- **Full Backup Strategy:** A full backup strategy involves creating a complete copy of all data on a system or device. This type of backup takes longer to perform and requires more storage space than other backup strategies, but it offers comprehensive data protection. Full backups are typically performed on a periodic basis, such as weekly or monthly.
- **Incremental Backup Strategy:** An incremental backup strategy involves backing up only the data that has changed since the last backup. This type of backup is faster and requires less storage space than full backups. Incremental backups can be performed on a daily basis or more frequently, depending on the amount of data generated.
- **Differential Backup Strategy:** A differential backup strategy involves copying all data that has changed since the last full backup. This type of backup is faster than full backups but slower than incremental backups. Differential backups are typically performed on a periodic basis, such as weekly.
- **Mirror Backup Strategy:** A mirror backup strategy involves creating an exact copy of the data on a system or device. This type of backup is useful for disaster recovery, as it provides an exact replica of the data that can be used to restore a system in case of a disaster.
- **Hybrid Backup Strategy:** A hybrid backup strategy involves combining two or more backup strategies to create a

comprehensive backup and recovery plan. For example, an organization might use a full backup strategy once a month, an incremental backup strategy daily, and a mirror backup strategy for critical systems.

- **Offsite Backup Strategy:** An offsite backup strategy involves storing backups in a location that is physically separate from the primary data center. This type of backup strategy provides additional protection against disasters that may affect the primary data center.
- **Cloud Backup Strategy:** A cloud backup strategy involves storing backups in the cloud. This type of backup strategy provides additional flexibility and scalability, as well as offsite storage.
- **Tape Backup Strategy:** A tape backup strategy involves storing backups on tape. This type of backup strategy is reliable and cost-effective but requires more manual intervention than other backup strategies.

When choosing a backup strategy, organizations should consider factors such as the amount of data generated, the criticality of the data, the budget, and the resources available for backup and recovery. A comprehensive backup strategy should include both full and incremental backups, as well as offsite storage or cloud backup to provide additional protection against disasters. Regular testing of backups is also essential to ensure that data can be restored in case of a disaster or system failure.

12.7 DOWNLOADING AND MANAGEMENT OF THIRD PARTY SOFTWARE

Third-party software refers to software that is developed by a company or individual that is not the original manufacturer or developer of a particular software or hardware product. Third-party software can be used to add new features or functionality to existing software, or to extend the capabilities of hardware devices.

Examples of third-party software include plugins, add-ons, and extensions for web browsers, as well as software applications such as productivity tools, security software, and media players. Third-party software

can be purchased or downloaded for free from a variety of sources, including software developers' websites, app stores, and other online marketplaces.

While third-party software can provide many benefits, including increased functionality and improved productivity, it can also pose a security risk if not properly managed. Some third-party software may contain vulnerabilities or be intentionally designed to deliver malware or other malicious software to a user's computer. It is important to carefully evaluate third-party software before downloading or installing it, and to follow best practices for managing and updating software to ensure that it remains secure.

Downloading and managing third-party software can present several security risks, including the risk of downloading malware or other malicious software. Here are some best practices for downloading and managing third-party software:

- **Choose Reputable Sources for Downloads:** The first step in downloading and managing third-party software is to choose reputable sources for downloads. Reputable sources include official websites of software vendors, popular download portals like CNET or Softonic, and app stores like Google Play or Apple App Store. We should avoid downloading software from unknown or untrusted sources, as they may contain malware or other malicious code that can compromise the security of your system.
- **Verify Software Authenticity:** Before downloading third-party software, it is important to verify its authenticity. This involves checking whether the software is legitimate and not a fake or counterfeit version that can contain malware. To verify software authenticity, we can look for digital signatures or hash values provided by the software vendor. Digital signatures are cryptographic tools that verify the identity of the software vendor and ensure the integrity of the software package. Hash values are unique identifiers that ensure the software package has not been tampered with during the download process.
- **Check Compatibility and System Requirements:** Before downloading and installing third-party software, it is important to check its compatibility and system requirements. We need to ensure

that the software is compatible with our operating system and meets the minimum system requirements, such as processor speed, RAM, and disk space. Installing software that is not compatible with your system can cause compatibility issues and may compromise system performance or stability.

- **Use Antivirus and Anti-Malware Software:** Using antivirus and anti-malware software is essential to protect your system from malware and other security threats that may be present in third-party software. We need to ensure that our antivirus software is up-to-date and set to perform regular scans of your system. Antivirus and anti-malware software can detect and remove malicious code that may be present in third-party software, reducing the risk of compromise or data loss.
- **Regularly Update Third-Party Software:** Regularly updating third-party software is important to ensure that it remains secure and free from vulnerabilities. Software vendors release updates and patches to address security issues and improve functionality, and it is important to install them as soon as they become available. Set up automatic updates for third-party software to ensure that updates are installed promptly. Regularly check for updates manually if automatic updates are not available.
- **Remove Unused and Unnecessary Software:** Removing unused and unnecessary third-party software is important to reduce the attack surface of your system and minimize the risk of security breaches. Unused software can create vulnerabilities that can be exploited by attackers, and it can also consume system resources and affect system performance. Regularly review the software installed on your system and remove any software that is not required or no longer in use. This can be done using the control panel or third-party software uninstaller tools.
- **Use Virtualization or Sandboxing:** Virtualization or sandboxing is a technique that isolates third-party software from the host system, reducing the risk of compromise or data loss. Virtualization involves creating a virtual environment in which software can run, while

sandboxing involves restricting the access of software to system resources. Virtualization or sandboxing can be used to test new software or run potentially risky software, such as malware analysis tools, in a controlled environment without affecting the host system.

- **Implement Access Controls:** Implementing access controls is important to ensure that only authorized users can download and install third-party software. Access controls can include password protection, two-factor authentication, and role-based access control.



CHECK YOUR PROGRESS

Q1. State True or False

a) Router is an endpoint device.

b) Encrypting data on a device makes it impossible for hackers to access the data.

c) Security patches are updates released by software vendors to fix known security vulnerabilities.

d) It is not necessary to back up data regularly because modern hard drives are very reliable.

e) Incremental backups only copy files that have been modified or created since the last backup.

f) Third-party software is always free to download and use.

g) All third-party software is compatible with all devices and software platforms.



12.8 LET US SUM UP

- Endpoint device security refers to the protection of individual devices such as desktops, laptops, smartphones, and tablets from potential cyber threats.
- Endpoint device security measures include implementing strong passwords, regularly updating software, using antivirus software, and

restricting access to sensitive data.

- Challenges in mobile security include the variety of mobile devices and operating systems, the increasing complexity of mobile apps, and the vulnerability of mobile networks to attacks.
- Countermeasures for mobile device security include implementing device encryption, using strong passwords, keeping software up-to-date, using mobile device management (MDM) solutions, and training users on safe mobile device usage.
- A password policy is a set of rules and guidelines designed to ensure that passwords used by individuals are strong, secure, and less vulnerable to cyber attacks.
- Security patch management involves the process of identifying, acquiring, testing, and installing software patches to address vulnerabilities and improve the security of an organization's IT systems.
- Best practices for security patch management include prioritizing patches based on risk level, testing patches before deployment, keeping a detailed inventory of assets, and regularly monitoring for new vulnerabilities.
- Data backup is the process of creating duplicate copies of important data and storing them securely to protect against data loss due to human error, system failures, or cyber attacks.
- Awareness of installing third-party software involves researching the software beforehand, verifying the source, reading the terms and conditions, and using antivirus software to protect against potential malware or viruses.



12.9 FURTHER READINGS

1) "Computer Security Fundamentals" by Chuck Easttom
2) "Network Security Essentials: Applications and Standards" by William Stallings
3) "Introduction to Computer Security" by Michael T. Goodrich and Roberto Tamassia

4) "Principles of Computer Security: CompTIA Security+ and Beyond" by Wm. Arthur Conklin, Greg White, and Chuck Cothren

5) "Computer Security Handbook" by Seymour Bosworth, Michel E. Kabay, and Eric Whyne

6) "Foundations of Computer Security" by David Salomon and Giovanni Motta

7) "Cybersecurity Essentials" by Charles J. Brooks and Christopher Grow



12.10 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q. No. 1:

a) True

b) False

c) True

d) False

e) True

f) False

g) False



12.11MODEL QUESTIONS

Q1. What is the difference between antivirus and anti-malware software?

Q2. What are the benefits of using strong passwords?

Q3. What is two-factor authentication?

Q4. What is the purpose of encryption on mobile devices?

Q5. What are the different kinds of attacks in mobile devices?

Q6. What is the difference between a security patch and a software update?

Q7. What is a patch management system and how does it work?

Q8. Discuss some common backup strategies.

*** ***** ***

UNIT 13: DIGITAL DEVICE SECURITY II

UNIT STRUCTURE

13.1 Learning Objectives

13.2 Introduction

13.3 Device Security Policy

13.4 Cyber Security Best Practices

13.5 Significance of Host Firewall and Ant-virus

13.6 Management of Host firewall and Anti-virus

13.7 Let Us Sum Up

13.8 Further Readings

13.9 Answers to Check Your Progress

13.10 Model Questions

13.1 LEARNING OBJECTIVES

After goingthrough this unit, you will be able to:

- understand the basic concepts of Digital Device Security Policy
- use best practices for cyber security
- understand the concept of firewall and antivirus software

13.2 INTRODUCTION

In the last unit, we learned about end-point device and mobile phone security. We also understood the importance of password policy and data backup in the last unit.

In this unit, we are going to learn about basic concepts of device security policy, best practices for cyber security and concepts of firewall and antivirus software.A device security policy is a set of rules and guidelines that dictate how devices within an organization should be secured. It encompasses the processes, procedures, and technologies that are used to safeguard devices from unauthorized access, data theft, malware, and other cyber threats. Again, a firewall is a network security device that monitors and controls incoming and outgoing network traffic. It acts as a barrier

between a trusted network and an un-trusted network (such as the internet) and can be hardware or software-based. Firewalls are used to prevent unauthorized access to a network, block malicious traffic, and protect against cyber threats such as malware, viruses, and hacking attempts.Antivirus software is a program designed to detect, prevent, and remove malicious software (malware) from a computer or network. It scans files and incoming/ outgoing network traffic for known malware signatures, and uses heuristics and behavioral analysis to detect unknown malware. Antivirus software is an essential component of a comprehensive cybersecurity strategy and should be regularly updated to ensure it can detect the latest threats. In the next unit, we will discuss about Wi-Fi security in detail.

13.3 DEVICE SECURITY POLICY

Device security policy is the set of guidelines and procedures that an organization implements to ensure the security of devices such as computers, mobile phones, tablets, and other digital devices. The device security policy is crucial in protecting an organization's digital assets, which can be compromised by unauthorized access, malware, and other cyber threats. In this unit, we will discuss the importance of device security policy, the elements that make up a robust device security policy, and the best practices for implementing and maintaining a device security policy. The proliferation of digital devices and the increase in cyber threats have made device security policy a critical concern for organizations of all sizes. A robust device security policy helps an organization to protect its digital assets. Digital assets such as customer data, intellectual property, and financial information are essential to an organization's success. A device security policy helps protect these assets by preventing unauthorized access, data theft, and other cyber threats. Again, many industries are subject to regulatory requirements that mandate the protection of sensitive information. A device security policy helps organizations comply with these requirements and avoid costly penalties. Another advantage of device security policy is that it maintains customer trust. Customers expect their data to be secure when

they interact with an organization. A device security policy helps maintain customer trust by ensuring that sensitive data is protected.

Elements of Device Security Policy

A comprehensive device security policy should address the following elements:

- **Access control :** The policy should define who has access to devices and what level of access they have. Access should be restricted to authorized personnel, and authentication mechanisms such as passwords or biometrics should be used to ensure that only authorized users can access devices.
- **Device configuration :** The policy should define how devices are configured to ensure security. This includes the use of encryption, firewalls, and other security measures to protect against malware, data theft, and other cyber threats.
- **Monitoring and logging :** The policy should define how devices are monitored and logged to detect and respond to security incidents. This includes monitoring for suspicious activity, logging events, and analyzing logs to identify potential threats.
- **Incident response :** The policy should define how security incidents are reported, investigated, and responded to. This includes procedures for containing incidents, investigating their cause, and taking corrective actions to prevent similar incidents from occurring in the future.
- **Data protection :** The policy should define how data is protected on devices. This includes the use of encryption, backups, and secure deletion to prevent data loss or theft.

Best Practices for Implementing and Maintaining Device Security Policy

- Implementing and maintaining a device security policy can be a daunting task, but the following best practices can help:
- **Conduct a risk assessment :** Before implementing a device security policy, organizations should conduct a risk assessment

to identify the threats and vulnerabilities that exist in their environment. This will help them to develop a policy that addresses their specific risks.

- **Involve all stakeholders :** A device security policy should involve all stakeholders, including IT staff, management, and employees. This ensures that everyone is aware of the policy and their responsibilities in implementing it.
- **Regularly update the policy :** A device security policy should be regularly updated to address new threats and vulnerabilities as they emerge. This ensures that the policy remains relevant and effective in protecting the organization's digital assets.
- **Provide training :** All employees should receive training on the device security policy to ensure that they understand the policy and their responsibilities in implementing it. Training should be provided regularly to keep employees up to date on new threats and changes to the policy.
- **Use automation :** Automation can help organizations to implement and maintain their device security policy more efficiently. For example, automated patch management can ensure that devices are kept up to date with the latest security patches.

13.4 CYBER SECURITY BEST PRACTICES

Cyber security best practices refer to a set of procedures, processes, and actions that organizations can implement to protect their digital assets from cyber threats. Cyber security best practices involve a combination of technical, organizational, and human factors. Technical best practices include the use of firewalls, antivirus software, encryption, and other security measures to protect networks, devices, and data. Organizational best practices include the development and implementation of security policies, procedures, and controls to manage cyber security risks. Human factors involve educating employees on cyber security risks, implementing access controls, and promoting a culture of security awareness. Overall, cyber

security best practices are essential in protecting an organization's digital assets from cyber threats such as phishing attacks, malware, and data breaches.

The framework for implementing cybersecurity best practices is divided into the following four main components:

- **Identify:** This component involves identifying the assets, vulnerabilities, and risks associated with an organization's digital environment. By conducting a thorough risk assessment, organizations can develop a comprehensive understanding of their cybersecurity risks and develop a plan to address them.
- **Protect:** This component involves implementing security measures to protect an organization's digital assets. This includes technical measures such as firewalls, encryption, and antivirus software, as well as organizational measures such as security policies and procedures.
- **Detect:** This component involves monitoring an organization's digital environment for signs of cyber threats. This includes implementing monitoring tools and techniques to detect anomalies and potential security incidents.
- **Respond:** This component involves responding to security incidents and minimizing their impact. This includes having a plan in place to contain and mitigate security incidents, as well as conducting post-incident analysis to prevent similar incidents from occurring in the future.

Now, let us take a closer look at each component and the best practices associated with it.

1. Identify

The first component of the framework involves identifying the assets, vulnerabilities, and risks associated with an organization's digital environment. This includes:

- **Conducting a Risk Assessment:** A risk assessment is an essential step in identifying an organization's cybersecurity risks.

This involves identifying assets, assessing vulnerabilities, and evaluating the likelihood and impact of potential threats. By conducting a risk assessment, organizations can develop a comprehensive understanding of their cybersecurity risks and develop a plan to address them.

- **Developing Security Policies and Procedures:** Security policies and procedures provide a framework for implementing cybersecurity best practices. These policies and procedures should address access control, password management, incident response, and other cybersecurity issues.
- **Implementing Access Controls:** Access controls are essential in preventing unauthorized access to an organization's digital assets. This includes implementing user authentication, authorization, and accountability measures to ensure that only authorized personnel have access to sensitive information.
- **Conducting Third-Party Risk Assessments:** Third-party vendors and partners may have access to an organization's digital assets. Therefore, it is essential to conduct third-party risk assessments to ensure that they are adhering to cybersecurity best practices.

2. Protect

The second component of the framework involves implementing security measures to protect an organization's digital assets. This includes:

- **Implementing Technical Measures:** Technical measures such as firewalls, antivirus software, encryption, and intrusion detection and prevention systems (IDPS) are essential in protecting an organization's digital assets from cyber threats.
- **Implementing Organizational Measures:** Organizational measures such as security policies, procedures, and controls are essential in protecting an organization's digital assets. This includes implementing data backup and recovery procedures, conducting regular security audits, and implementing employee training programs.

- **Implementing Physical Security Measures:** Physical security measures such as access control systems, CCTV, and security guards are essential in preventing unauthorized physical access to an organization's digital assets.
- **Implementing Data Protection Measures:** Data protection measures such as data encryption, data masking, and data loss prevention (DLP) are essential in protecting an organization's sensitive data.

3. Detect

The third component of the cybersecurity best practices framework is "Detect". This component involves monitoring an organization's digital environment for signs of cyber threats. This includes implementing monitoring tools and techniques to detect anomalies and potential security incidents.

There are several best practices that organizations can implement in the "Detect" component of the framework. Some of them are:

- **Implement Continuous Monitoring:** Continuous monitoring is the process of monitoring an organization's digital environment in real-time to detect security incidents. This includes monitoring network traffic, log files, and user activity. By implementing continuous monitoring, organizations can detect security incidents as they occur, minimizing the impact of the incident.
- **Implement Security Information and Event Management (SIEM):** SIEM is a software solution that collects, aggregates, and analyzes security events from various sources within an organization's digital environment. SIEM provides real-time threat detection, incident response, and compliance reporting. By implementing SIEM, organizations can detect security incidents in real-time and respond quickly to minimize their impact.
- **Implement Intrusion Detection and Prevention Systems (IDPS):** IDPS is a security solution that detects and prevents security incidents. IDPS can detect and prevent a range of security

incidents, including network attacks, malware, and insider threats. By implementing IDPS, organizations can detect and prevent security incidents before they cause damage.

- **Conduct Vulnerability Scanning:** Vulnerability scanning is the process of identifying vulnerabilities in an organization's digital environment. This includes scanning for vulnerabilities in software, hardware, and network devices. By conducting vulnerability scanning, organizations can identify vulnerabilities and take proactive measures to address them before they are exploited by attackers.
- **Implement Endpoint Detection and Response (EDR):** EDR is a security solution that monitors endpoints such as desktops, laptops, and mobile devices for signs of security incidents. EDR can detect and prevent a range of security incidents, including malware, ransomware, and phishing attacks. By implementing EDR, organizations can detect security incidents at the endpoint, minimizing their impact.
- **Implement Threat Intelligence:** Threat intelligence is information about potential cyber threats. By implementing threat intelligence, organizations can stay up-to-date on the latest cyber threats and take proactive measures to protect their digital assets.
- **Conduct Regular Security Audits:** Regular security audits can help organizations identify security vulnerabilities and gaps in their security controls. By conducting regular security audits, organizations can identify areas where security controls need to be strengthened.

4. Respond

The fourth component of the cybersecurity best practices framework is "Respond". This component involves responding to security incidents in a timely and effective manner to minimize the impact of the incident.

There are several best practices that organizations can implement in the "Respond" component of the framework:

- **Develop an Incident Response Plan:** An incident response plan outlines the steps that an organization will take in the event of a security incident. The plan should include procedures for detecting, reporting, analyzing, containing, and recovering from security incidents. By developing an incident response plan, organizations can respond quickly and effectively to security incidents.
- **Conduct Tabletop Exercises:** Tabletop exercises are simulations of security incidents that allow organizations to practice their incident response plans. By conducting tabletop exercises, organizations can identify areas where their incident response plans need improvement and ensure that all stakeholders understand their roles and responsibilities during a security incident.
- **Establish a Security Operations Center (SOC):** A SOC is a centralized team responsible for monitoring and responding to security incidents. The SOC should be staffed with trained security professionals who can detect, investigate, and respond to security incidents. By establishing a SOC, organizations can respond quickly and effectively to security incidents.
- **Implement Incident Response Tools:** Incident response tools include forensic analysis tools, malware analysis tools, and incident response platforms. These tools can help organizations investigate security incidents and respond quickly to minimize their impact.
- **Develop Communication Procedures:** Communication procedures should be established for notifying stakeholders, including customers, employees, and regulatory bodies, of security incidents. The communication procedures should include clear and concise messaging that outlines the impact of the incident and the steps that the organization is taking to mitigate the impact.
- **Coordinate with Law Enforcement:** In some cases, security incidents may involve criminal activity. Organizations should coordinate with law enforcement to ensure that the incident is properly investigated and prosecuted.

- **Conduct Post-Incident Analysis:** After a security incident, organizations should conduct a post-incident analysis to identify areas where their incident response plan needs improvement. The post-incident analysis should include a review of the incident response plan, incident response tools, communication procedures, and coordination with law enforcement.

13.5 SIGNIFICANCE OF HOST FIREWALL AND ANT-VIRUS

In recent worlds, protecting our sensitive data from unwanted and unauthorized sources is a big challenge. There are various tools and devices that provide different levels of security and help protect our private data. One such tool is a firewall, which prevents unauthorized access and protects our computers and data. A firewall can be defined as a special type of network security device or software that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between the internal private network and external resources such as the public Internet. The main purpose of a firewall is to protect your computer from viruses and attacks by allowing non-threatening traffic and blocking malicious or unwanted data traffic. A firewall is network security tools that filters network traffic and helps users prevent malware from accessing the Internet on an infected computer.

One of the most problematic questions is whether the firewall is hardware or software. As mentioned above, a firewall can be a network security device or a software program on a computer. This means that there are two layers of firewalls, hardware and software, although it is better to have both. Each format (firewall implemented as hardware or software) has different functions but the same purpose. A hardware firewall is a physical device that connects a computer network to a gateway. For example, a broadband router. A software firewall, on the other hand, is a simple program installed on a computer that operates through port numbers and other installed software.

Additionally, there are cloud-based firewalls. They are often called FaaS

(Firewall as a Service). One of the main advantages of using cloud-based firewalls is that they can be centrally managed. Like hardware firewalls, cloud-based firewalls are known to provide perimeter security.

Some of the important risks of not having a firewall are:

- Unauthorized access: Hackers can exploit network vulnerabilities to gain access to confidential information such as customer data, financial information, and intellectual property.
- Malware attacks: Malware such as viruses, worms, and Trojans can infect a network and cause damage to systems, corrupt data, or steal sensitive information.
- Denial-of-Service (DoS) attacks: DoS attacks can flood a network with traffic, causing it to crash and preventing legitimate users from accessing the network.
- Man-in-the-middle (MITM) attacks: MITM attacks involve intercepting network traffic to steal sensitive information or modify data.
- Phishing attacks: Phishing attacks involve tricking users into divulging sensitive information such as passwords or login credentials, often through fake emails or websites.
- Data leakage: Without a firewall, there is no protection against data leakage, which can occur when employees accidentally or intentionally share sensitive data outside of the network.
- Compliance violations: Many regulatory requirements, such as the Payment Card Industry Data Security Standard (PCI DSS), mandate the use of firewalls to protect sensitive information. Failure to comply with these regulations can result in fines, legal action, and damage to the organization's reputation.

How does a firewall work?

Firewall systems analyze network traffic according to predefined rules. It then filters the traffic and prevents this traffic from un-trusted or suspicious sources. It only allows incoming traffic that it is configured to accept.

Typically, a firewall blocks network traffic at an entry point to a computer, called a gateway. Firewalls accomplish this task by allowing or blocking specific packets (communication units that pass through a digital network) based on predefined security rules.

Incoming traffic is only allowed via IP addresses or trusted sources.

Functions of Firewall

A firewall acts as a gatekeeper. It scans every attempt to access our operating system and blocks traffic from unwanted or unrecognized sources. Since a firewall acts as a barrier or filter between computer systems and other networks (i.e. the public internet), we can think of it as a traffic controller. Therefore, the main function of a firewall is to protect our network and information by controlling network traffic, preventing unwanted incoming network traffic and verifying access by evaluating network traffic to detect malicious content such as hackers and malware. In general, most operating systems (for example, the Windows operating system) and security software come with built-in firewall support. It is therefore a good idea to ensure that these options are enabled. Additionally, we can configure system security settings to update automatically when available. The firewall has become so powerful and it includes the various built-in features like:

- Network Threat Prevention
- Application and Identity-Based Control
- Hybrid Cloud Support
- Scalable Performance
- Network Traffic Management and Control
- Access Validation
- Record and Report on Events

When it comes to network security, firewalls are considered the first line of defense. But the question is whether these firewalls are strong enough to protect our devices against cyberattacks. The answer is probably “no”. It is recommended to use a firewall system when using the Internet. However, it is important to use other defense systems to help protect the network and

the data stored on your computer. With ever-evolving cyber threats, a firewall shouldn't be the only consideration for securing your home network.

The importance of using a firewall as a security system is obvious; however, firewalls have some limitations:

- **Incomplete protection:** Firewalls are designed to protect against certain types of cyber threats, such as unauthorized access to a network or malicious data packets. However, they cannot protect against all types of cyber threats, such as social engineering attacks or phishing scams.
- **Overreliance:** Many organizations may over-rely on firewalls as a primary means of cybersecurity, without implementing additional measures such as antivirus software or intrusion detection systems. This can create a false sense of security and leave the organization vulnerable to other types of attacks.
- **Misconfiguration:** Firewalls must be properly configured to be effective, and even a small misconfiguration can render the firewall ineffective. This can be a problem for organizations that do not have dedicated IT staff or do not have the expertise to properly configure a firewall.
- **Vulnerabilities:** Like any software, firewalls are not immune to vulnerabilities and may contain exploitable flaws that can be used by attackers to bypass the firewall. It is important to keep firewalls up-to-date with the latest security patches to minimize the risk of vulnerabilities.
- **Insider threats:** Firewalls are designed to protect against external threats, but they may not be effective against insider threats such as employees or contractors who have legitimate access to the network. Insider threats can bypass firewalls by using legitimate credentials or exploiting vulnerabilities in the network.
- **Cost:** Firewalls can be expensive to implement and maintain, particularly for small and medium-sized businesses. This can be a barrier for organizations that do not have the budget or resources to implement a comprehensive cybersecurity strategy.

Organizations must be aware of these limitations and implement additional measures to address other types of cyber threats, such as antivirus software, intrusion detection systems, and employee training.

Types of Firewall

There are several types of firewalls available, each with their own unique characteristics and capabilities. Here are some of the most common types of firewalls:

1. **Packet Filtering Firewalls:** This is the most basic type of firewall that examines incoming and outgoing packets of data and allows or blocks them based on predetermined rules. Packet filtering firewalls work at the network layer of the OSI model and can only filter traffic based on IP address, port number, and protocol type.
2. **Stateful Inspection Firewalls:** Stateful inspection firewalls are more advanced than packet filtering firewalls as they not only inspect incoming and outgoing packets but also track the state of each connection to ensure that it is legitimate. These firewalls work at the network layer and can also inspect traffic at the transport layer of the OSI model.
3. **Application Firewalls:** Application firewalls work at the application layer of the OSI model and can inspect traffic at the application level, such as HTTP or FTP. This type of firewall can detect and block specific types of traffic, such as SQL injection attacks.
4. **Next-Generation Firewalls (NGFW):** NGFWs are advanced firewalls that combine the capabilities of packet filtering, stateful inspection, and application firewalls with advanced threat detection and prevention techniques. NGFWs can perform deep packet inspection and detect and block malware, viruses, and other advanced threats.
5. **Proxy Firewalls:** Proxy firewalls act as an intermediary between clients and servers, filtering traffic based on application-specific rules. Proxy firewalls can also provide additional security features such as content filtering and data loss prevention.

6. **Cloud Firewalls:** Cloud firewalls provide network security for cloud-based applications and services. These firewalls are hosted in the cloud and can be managed centrally, making them ideal for distributed environments.

Antivirus Software:

Just as we humans can get infected and get sick, our computers can get infected when connected to the internet. Viruses can infiltrate our computers through things we download from the Internet, such as emails or files copied online. Viruses can destroy our data by erasing it or making it unusable and can also affect the performance of our computer by slowing it down considerably. Viruses can also re-send our confidential data to other people or allow someone to remotely control our computer and use it for their own purposes.

Antivirus software, also known as antimalware software, is a computer program used to prevent, detect, and remove malware. The antivirus software was originally developed to detect and remove computer viruses, hence its name. However, as more malware spread, antivirus software began to protect against other computer threats. Some products also include protection against malicious URLs, spam, and phishing. antivirus software uses various techniques to detect and remove malware from computer systems. Some of the key technologies used by modern antivirus programs include:

- **Signature-based detection:** This technique involves comparing the files on a computer system to a database of known malware signatures. When a file matches a known signature, the antivirus program will quarantine or remove the file from the system.
- **Heuristic-based detection:** This technique involves analyzing the behavior of files on a computer system to detect potentially malicious behavior. Antivirus software may use artificial intelligence or machine learning algorithms to detect new or unknown threats based on their behavior.
- **Behavioral-based detection:** This technique involves analyzing

the behavior of processes on a computer system to detect potentially malicious activity. Antivirus software may monitor processes for signs of suspicious activity, such as attempting to modify system files or communicating with known malicious servers.

- **Sandboxing:** This technique involves running potentially malicious code in a virtual environment to observe its behavior. This allows antivirus software to detect new or unknown threats that may not be detected by signature-based or heuristic-based detection.
- **Machine learning:** This technique involves training algorithms to identify malware based on patterns and characteristics of known malware. Machine learning algorithms can continuously learn and adapt to new threats, making them effective at detecting and preventing new and unknown threats.
- **Cloud-based detection:** This technique involves uploading suspicious files to a cloud-based server for analysis. The server can use more powerful hardware and machine learning algorithms to detect and identify potential threats.

Antivirus software typically consists of several components, including real-time scanners, quarantine managers, and update managers. Real-time scanners run in the background and constantly monitor files and processes on your computer system for signs of malicious activity. If the scanner detects a potential threat, it alerts the user and takes action to quarantine or delete the file. The quarantine administrator is responsible for managing and quarantining files that have been detected as potentially malicious. Quarantined files are usually stored in a safe place so that they cannot damage the system or spread to other files. The update manager is responsible for keeping antivirus software up to date with the latest malware definitions and detection technologies. Antivirus software must be updated regularly to be effective against emerging threats. In addition to these basic components, many antivirus programs include other features, such as firewalls, web filtering, and email scanning. These features provide an additional layer of protection against cyber threats.

Firewalls and antivirus software are both important components of a comprehensive cybersecurity strategy, but they serve different purposes and have different functions. Firewalls are network security devices that are designed to monitor and filter incoming and outgoing network traffic. They can be implemented in both hardware and software forms, and they work by examining data packets and determining whether to allow or block them based on a set of predetermined rules. Firewalls can block incoming connections from known malicious sources, prevent unauthorized access to sensitive data, and prevent malware from communicating with remote servers.

Antivirus software, on the other hand, is designed to detect and remove malicious software, or malware, from a computer system. Antivirus software scans files and directories for known malware signatures or behavior, and can also use heuristics to detect unknown or zero-day malware. Antivirus software can detect and remove viruses, worms, Trojans, and other types of malware from a computer system. While both firewalls and antivirus software are essential components of a comprehensive cybersecurity strategy, they serve different purposes and have different functions. Firewalls focus on preventing unauthorized access to a network, while antivirus software focuses on detecting and removing malware from a computer system. Organizations should implement both firewalls and antivirus software to ensure comprehensive protection against cyber threats.



CHECK YOUR PROGRESS

Q1. State True or False

a) Access controls are not an essential component of device security policy.

b) Implementing a backup and recovery plan is not essential for maintaining device security policy.

c) Security Information and Event Management (SIEM) provides real-time threat detection, incident response, and compliance reporting.

d) Antivirus software is not necessary if the host firewall is properly configured.

e) Antivirus software can protect against zero-day attacks.

f) Packet-filtering firewalls inspect the contents of each packet passing through the firewall.

g) It is not necessary to monitor host firewall logs.

h) Cloud firewalls provide network security for cloud-based applications and services.

13.6 MANAGEMENT OF HOST FIREWALL AND ANTI-VIRUS

The management of host firewall and antivirus software is essential for maintaining the security and integrity of an organization's IT infrastructure. Host firewalls provide an additional layer of protection against malicious traffic and unauthorized access, while antivirus software helps to detect and remove malware that can compromise systems and data. Effective management of these security measures ensures that devices and networks are protected from cyber threats, such as viruses, ransomware, and phishing attacks. Regular updates and patches are crucial to keep up with the latest threats, and continuous monitoring and maintenance are necessary to ensure that the firewall and antivirus software are functioning as intended. Without proper management, the organization's IT assets are vulnerable to compromise, leading to potential data loss, system downtime, and financial losses.

Effective management of host firewalls

Effective management of host firewalls is essential for maintaining network security. Here are some best practices for managing host firewalls:

- **Regularly Update Firewall Rules:** Firewall rules should be regularly updated to ensure that they reflect the current needs of the organization and provide adequate protection against the latest security threats. This includes removing outdated rules and

adding new rules to address emerging threats.

- **Enforce Least Privilege:** Host firewalls should be configured to enforce the principle of least privilege, which means that only necessary ports, protocols, and services are allowed through the firewall. This reduces the attack surface and minimizes the risk of unauthorized access.
- **Monitor Firewall Logs:** Firewall logs should be monitored regularly to identify suspicious activity and potential security breaches. This includes reviewing logs for denied connections, failed login attempts, and other indicators of malicious activity.
- **Implement Network Segmentation:** Network segmentation is the practice of dividing a network into smaller subnetworks to limit the impact of a security breach. Host firewalls can be used to enforce segmentation by restricting traffic between different segments of the network.
- **Harden the Firewall Configuration:** Firewall configurations should be hardened to prevent unauthorized changes and reduce the risk of misconfiguration. This includes disabling unnecessary services, using strong authentication, and enabling encryption for remote access.
- **Regularly Test Firewall Security:** Firewall security should be regularly tested to ensure that it is effective in detecting and preventing attacks. This includes conducting vulnerability scans and penetration testing to identify weaknesses in the firewall configuration.

Effective management of host firewalls requires regular maintenance, monitoring, and testing to ensure that they provide adequate protection against the latest security threats. By following these best practices, organizations can help ensure the integrity and confidentiality of their networks and data.

Management of antivirus software is essential for maintaining the security of computer systems and networks. Here are some best practices for managing antivirus software:

- **Regularly Update Antivirus Software:** Antivirus software should be updated regularly to ensure that it can detect and protect against the latest malware threats. This includes updating virus definitions, software patches, and other security updates.
- **Configure Antivirus Software Settings:** Antivirus software settings should be configured to meet the specific needs of the organization. This includes setting up scheduled scans, configuring real-time protection, and setting up email and web filtering.
- **Monitor Antivirus Software Alerts:** Antivirus software alerts should be monitored regularly to identify potential security breaches. This includes reviewing alerts for malware detections, failed scans, and other indicators of malicious activity.
- **Perform Regular Scans:** Regular scans should be performed on all systems to detect and remove malware. This includes scheduled scans of all systems and on-demand scans of specific files or directories.
- **Conduct User Training:** User training is important to educate employees on safe browsing and email practices to reduce the risk of malware infections. This includes training on how to recognize phishing emails, how to avoid downloading and installing malware, and how to report suspected security incidents.
- **Test Antivirus Software Security:** Antivirus software security should be regularly tested to ensure that it is effective in detecting and preventing malware. This includes conducting penetration testing and other security tests to identify weaknesses in the antivirus configuration.

Overall, effective management of antivirus software requires regular maintenance, monitoring, and testing to ensure that it provides adequate protection against the latest malware threats. By following these best practices, organizations can help ensure the integrity and confidentiality of their computer systems and data.

Effective management of antivirus software

Effective management of antivirus software is crucial for maintaining the security and integrity of an organization's IT infrastructure. Here are some best practices for managing antivirus software:

- Regularly update the antivirus software to ensure it can detect the latest threats.
- Schedule regular scans of all devices and systems to detect any malware that may have been missed.
- Configure the antivirus software to automatically update and scan devices in real-time.
- Use a centralized management console to monitor antivirus activity across all devices and systems.
- Ensure that all devices and systems have the antivirus software installed and activated.
- Educate employees on how to recognize and avoid potential malware threats, such as phishing emails or suspicious attachments.
- Perform regular backups of critical data to prevent data loss in the event of a malware attack.
- Test the antivirus software's effectiveness by performing penetration testing or red teaming exercises.
- Consider using additional security measures, such as endpoint detection and response (EDR) or threat intelligence, to enhance the overall security posture.
- Regularly review and update the organization's antivirus policy and procedures to reflect changes in the threat landscape and business needs.



13.7 LET US SUM UP

- A device security policy is a set of guidelines and rules that govern the security of devices within an organization.

- Elements of a device security policy include password management, device encryption, regular software updates, and restrictions on device usage.
- Regularly review and update device security policy to incorporate current best practices and mitigate potential security risks.
- Develop and implement a comprehensive cybersecurity framework that addresses all aspects of security, including people, processes, and technology.
- Host firewall and antivirus are critical components of a layered defense strategy to protect against malware and unauthorized access, and to prevent or limit the impact of security incidents on the host system.
- Effective management of host firewall and antivirus requires regular updates, patches, monitoring, and configuration tuning to ensure optimal performance and protection against emerging threats.



13.8 FURTHER READINGS

1) "Computer Security Fundamentals" by Chuck Easttom
2) "Network Security Essentials: Applications and Standards" by William Stallings
3) "Introduction to Computer Security" by Michael T. Goodrich and Roberto Tamassia
4) "Firewalls and Internet Security: Repelling the Wily Hacker" by William R. Cheswick and Steven M. Bellovin



13.9 ANSWERS TO CHECK YOUR PROGRESS

Ans to Q. No. 1:

a) False
b) False
c) True
d) False

e) False

f) False

g) False

h) True



13.10 MODEL QUESTIONS

Q1. Discuss the elements of comprehensive device security policy.

Q2. What is a firewall, and how does it protect a network or system?

Q3. Discuss various types of firewall.

Q4. What is antivirus software, and how does it work to protect a system or network?

Q5. Differentiate firewall and antivirus software.

*** ***** ***

UNIT 14: WI-FI SECURITY

UNIT STRUCTURE

14.1 Learning Objectives

14.2 Introduction

14.3 Advantages of Using Wi-Fi

14.4 Threats of Using Wi-Fi

14.5 Types of Wi-Fi Network

14.6 Wi-Fi Types

14.7 Working of Wi-Fi

14.8 Setting Wi-Fi Security

14.9 Setting Wi-Fi Security in Android Mobile

14.10 Setting Wi-Fi Security in IOS Mobile

14.11 Let us Sum Up

14.12 Answer to Check Your Progress

14.13 Further Readings

14.14 Model Questions

14.1 LEARNING OBJECTIVES

After going through this unit, the learners will be able to:

- describe the advantages and threats of using Wi-Fi.
- identify different types of Wi-Fi networks and their characteristics.
- differentiate between various types of Wi-Fi, including 802.11a/b/g/n/ac/ax.
- explain how Wi-Fi works and the technology behind it.
- demonstrate the process of setting Wi-Fi security for a network.
- explain how to set Wi-Fi security on Android mobile devices.
- explain how to set Wi-Fi security on iOS mobile devices.

14.2 INTRODUCTION

In the last unit, we learned about device security policy and best practices for cyber security. We also discussed the significance and

management details regarding fire-well and anti-virus software. In this last unit of the course we will discuss about Wi-Fi security.

Without the need of physical connections or wires, Wi-Fi (short for "wireless fidelity") is a sort of wireless networking technology that enables devices to connect to the internet or other devices. Wi-Fi uses radio waves to send data between gadgets and a wireless access point (like a router), which serves as a conduit for connecting the gadgets to the internet. Wi-Fi is frequently used to connect a variety of devices, including computers, smartphones, tablets, and smart home appliances, to the internet in homes, workplaces, public places, and other areas. A variety of encryption techniques can be used to secure Wi-Fi networks against illegal access or data theft.

14.3 ADVANTAGES OF USING WI-FI

Let us look at some advantages of using Wi-Fi services:

- **Convenience:** Wi-Fi offers the benefit of wireless internet access from anywhere that is within the Wi-Fi network's coverage area.
- **Flexibility:** Wi-Fi enables you to roam about while maintaining an online connection without the use of cables or wires.
- **Support for many devices:** Wi-Fi networks enable several devices, including tablets, laptops, and smartphones, to connect to the internet simultaneously.
- **Economical:** Wi-Fi technology is frequently less expensive than traditional methods of connecting to the internet.
- **Security:** Wi-Fi networks offer a higher level of security than open internet access since they can be protected with passwords and encryption.
- **Quick internet access:** Wi-Fi networks can offer quick internet access, making it possible to download, play games, and stream high-definition videos.
- **Simple installation:** Putting up a Wi-Fi network is doable without specialist assistance.
- **Accessibility:** Users can easily access Wi-Fi networks from a

range of devices, making it simple for them to use their preferred device to access the internet.

- **Remote control:** With a Wi-Fi connection, many devices, including printers, security cameras, and smart home appliances, may be operated remotely.
- **Collaboration:** Collaboration is made possible via Wi-Fi networks, which make it simple for users to share files, work on projects, and interact with one another.

14.4 THREATS OF USING WI-FI

Let us look at the threats of using Wi-Fi:

- **Security risks:** Wi-Fi networks are susceptible to security breaches because hackers can quickly get access to them and steal sensitive information like passwords and credit card numbers.
- **Infections with malware:** Unsecured Wi-Fi networks are also susceptible to malware infections, including viruses, Trojan horses, and spyware, which can affect users' devices and jeopardise their security.
- **Identity theft:** By obtaining users' personal information, such as their name, address, and social security number, cybercriminals can exploit Wi-Fi networks to steal users' identities.
- **Network congestion:** When a Wi-Fi network is overloaded, it can lead to slower speeds, dropped connections, and other connectivity problems.
- **Improper content:** Accessing unsuitable or explicit content using public Wi-Fi networks can insult other users or perhaps be against the law.
- **Wi-Fi jamming:** Attackers can interfere with Wi-i signals by utilising jamming devices, which can lead to disruptions or prevent users from connecting to the network.
- Wi-fi networks can be exploited to track users' whereabouts and movements, jeopardising their security and privacy.

14.5 TYPES OF WI-FI NETWORK

There are several types of Wi-Fi networks, including:

- **Personal Area Network (PAN):** The smallest kind of Wi-Fi network is the Personal Area Network (PAN), which is generally used for communication between computers, tablets, and smartphones.
- **Local Area Network (LAN):** This kind of network connects devices to a central hub, like a router or access point, in small- to medium-sized enterprises and homes.
- **Wide Area Network (WAN):** A larger version of a LAN, a WAN is typically used to connect multiple LANs in different geographic locations.
- **Mesh Network:** To give Wi-Fi coverage over a bigger region, this kind of network comprises of numerous access points that talk to one another.
- **Hotspot:** A Wi-Fi hotspot is a public Wi-Fi network typically found in airports, coffee shops, and other public places.
- **Virtual Private Network (VPN):** A VPN is a safe way to establish an encrypted connection from a distant place to a network.
- **Ad Hoc Network:** Ad hoc networks are peer-to-peer networks without a central hub where devices connect to each other directly.

14.6 WI-FI TYPES

- **802.11a:** This Wi-Fi standard operates at a 5GHz frequency and can transfer data at a maximum speed of 54Mbps. Because of its limited range and higher cost, it is not as commonly utilised as other Wi-Fi protocols.
- **802.11b:** The earliest Wi-Fi standard is 802.11b, which uses a 2.4GHz frequency. With a maximum data transfer rate of 11Mbps, it is no longer in widespread usage.

- **802.11g:** With a top data transfer rate of 54Mbps, this Wi-Fi standard also operates at 2.4GHz. It has a large user base and works with older gadgets.
- **802.11n**: This Wi-Fi standard operates at both 2.4GHz and 5GHz frequencies and has a maximum data transfer rate of 600Mbps. It is the most widely used Wi-Fi standard and provides better coverage and faster speeds.
- **802.11ac**: The most recent Wi-Fi standard, 802.11ac, operates at a frequency of 5GHz. In comparison to 802.11n, it offers greater coverage and higher speeds, with a maximum data transmission rate of 1Gbps.
- **802.11ax**: Often referred to as Wi-Fi 6, this Wi-Fi standard has a maximum data transfer rate of up to 10Gbps and works at both 2.4GHz and 5GHz frequencies. In high-density settings like stadiums and airports, it offers higher network efficiency.



CHECK YOUR PROGRESS

1. Choose the correct option from the following:

   (a) What does Wi-Fi stand for?

   (i) Wired Fidelity (ii) Wireless Fidelity

   (iii) Wide Fidelity (iv) None of the above

   (b) What type of waves does Wi-Fi use to send data between devices?

   (i) Sound Waves (ii) Radio Waves

   (iii) Light Waves (iv) None of the above

   (c) What is the maximum data transfer rate for Wi-Fi 802.11n?

   (i) 11Mbps (ii) 54Mbps

   (iii) 600Mbps (iv) 1Gbps

(d) Which type of Wi-Fi network is used to connect multiple LANs in different geographic locations?

(i) PAN (ii) LAN

(iii) WAN (iv) Mesh Network

(e) What is the smallest type of Wi-Fi network used for communication between computers, tablets, and smartphones?

(i) PAN (ii) LAN

(iii) WAN (iv) Mesh Network

(f) Which Wi-Fi standard operates at a frequency of 5GHz and has a maximum data transmission rate of 1Gbps?

(i) 802.11a (ii) 802.11b

(iii) 802.11ac (iv) 802.11ax

(g) Which type of Wi-Fi network comprises of numerous access points that talk to one another to give Wi-Fi coverage over a bigger region?

(i) PAN (ii) LAN

(iii) WAN (iv) Mesh Network

(h) What is the benefit of using Wi-Fi for internet access?

(i) Quick internet access (ii) Remote control

(iii) Security (iv) All of the above

14.7 WORKING OF WI-FI

With the help of Wi-Fi, devices may connect with one another wirelessly and without the use of physical cords. Wi-Fi operates on the fundamental tenet that radio waves are used to transmit data.

Our device transmits a signal to the router, which serves as the network's nerve centre, when we join a Wi-Fi network. A radio signal that other devices can pick up is emitted when the router gets this signal. The electromagnetic waves that make up this radio signal are transmitted at a specified frequency.

We can access the internet or other network resources by having our

device pick up this radio signal and decode it. The Wi-Fi signal can pass through walls and other impediments, but the distance between our device and the router as well as any physical barriers in the way can have an impact on its strength and quality.

The frequency used by Wi-Fi networks varies based on the particular protocol being used. The two most popular Wi-Fi frequencies are 2.4 GHz and 5 GHz, with 2.4 GHz being utilised more frequently by older devices and 5 GHz by newer, higher-end ones.

14.8 SETTING WI-FI SECURITY

The basic steps for Wi-Fi security:

a) **Modify the default SSID and password:** Be sure to modify the router's default network name (SSID) and password. This will assist in preventing illegal access to our network.

b) **Use WPA2 encryption:** We should ensure that WPA2 is enabled on our Wi-Fi (Wi-Fi Protected Access 2). This offers robust encryption that aids in preventing unauthorised individuals from intercepting our data.

c) **Enable a strong password:** We need to make sure the password we set for our Wi-Fi network is secure. Employ a mix of symbols, numerals, and capital and lowercase letters.

d) **Update router firmware:** We should ensure that the firmware on our router is up to date. By doing this, we can be sure that our router is secure against known vulnerabilities.

e) **Turn off WPS:** On our router, we need to disable Wi-Fi Protected Setup (WPS). Hackers may take advantage of known flaws in this functionality.

f) **Disable remote administration:** On our router, we should disable remote administration. This will stop unauthorised individuals from remotely accessing your router.

g) **Use a firewall:** We need to make sure our router has a built-in firewall. This will help protect our network from unauthorized access.

h) **Monitor the network:** We need to keep an eye out for any strange behaviour on our network. This will enable us to recognise any possible security threats and take the necessary precautions.

By following these basic steps, we can create a secure Wi-Fi network that protects our data and devices from cyber threats.

14.9 SETTING WI-FI SECURITY IN ANDROID MOBILE

Let us look at the steps on how to set up Wi-Fi security in Android mobile:

Step 1: Open the Android device's settings menu.

Step 2: Tap on the "Wi-Fi" option.

Step 3: Find the Wi-Fi network we want to secure and tap on it.

Step 4: Tap on "Advanced" or "Network" settings.

Step 5: Choose the security type we want to use. The options available may depend on the network we are connecting to.

Step 6: Enter the password or other security credentials for the network.

Step 7: Save the settings.

It's important to secure the Wi-Fi connections to prevent unauthorized access to our personal information.

14.10 SETTING WI-FI SECURITY IN IOS MOBILE

To set Wi-Fi security on an iOS mobile device, we need to follow these steps:

Step 1: Open the "Settings" app on the device.

Step 2: Tap on "Wi-Fi".

Step 3: Find the Wi-Fi network we want to secure and tap on the information icon (i).

Step 4: Tap on "Configure DNS".

Step 5: Choose "Automatic".

Step 6: Go back to the Wi-Fi settings screen and tap on the same network.

Step 7: Enter the Wi-Fi network password, if required.

Step 8: Tap on "Security" and choose the appropriate security type

(WPA2 is recommended).

Step 9: Enter the security key/passphrase and tap on “Join”.

Step 10: The iOS device will now be connected to the Wi-Fi network with the selected security type.

Note: It is important to use a strong and unique password for your Wi-Fi network to ensure maximum security.



14.11 LET US SUM UP

- Wi-Fi is a wireless networking technology that allows devices to connect to the internet or other devices without physical connections or wires.
- Wi-Fi uses radio waves to send data between devices and a wireless access point, such as a router.
- Wi-Fi offers several advantages, including convenience, flexibility, support for multiple devices, and quick internet access.
- Wi-Fi networks can be secured with passwords and encryption, providing a higher level of security than open internet access.
- However, Wi-Fi networks are also susceptible to security risks, malware infections, identity theft, network congestion, and Wi-Fi jamming.
- There are various types of Wi-Fi networks, including Personal Area Network (PAN), Local Area Network (LAN), Wide Area Network (WAN), Mesh Network, Hotspot, Virtual Private Network (VPN), and Ad Hoc Network.
- There are different Wi-Fi types, such as 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax (Wi-Fi 6).
- Wi-Fi has become an essential part of our daily lives and is used in homes, workplaces, public places, and other areas.
- Wi-Fi enables users to access the internet from a range of devices, including computers, smartphones, tablets, and smart home appliances.
- Wi-Fi networks can be set up without specialist assistance, making it easy for users to install and use them.



14.12 ANSWER TO CHECK YOUR PROGRESS

Ans.to Q.No.1:

(a) (ii) (b) (ii) (c) (iii) (d) (iii)

(e) (i) (f) (iii) (g) (iv) (h) (iv)



14.13 FURTHER READINGS

1) Cyber Crime Impact in the New Millennium, by R. C Mishra, Auther Press. Edition 2010.
2) Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by SumitBelapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)
3) Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
4) Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
5) Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
6) Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
7) Fundamentals of Network Security by E. Maiwald, McGraw Hill.



14.14 MODEL QUESTIONS

Q.1: What is Wi-Fi and how does it work?

Q.2: What are the advantages of using Wi-Fi?

Q.3: How can Wi-Fi networks be secured against illegal access or data theft?

Q.4: Can Wi-Fi networks support multiple devices at the same time? If yes, how many?

Q.5: What are the economic benefits of using Wi-Fi technology?

Q.6: How can Wi-Fi networks offer a higher level of security than open internet access?

Q.7: What are the applications of Wi-Fi networks in smart home appliances?

Q.8: What are the threats of using Wi-Fi, and how can they be prevented?

Q.9: How can Wi-Fi networks be jammed, and what are the consequences?

Q.10: What are the different types of Wi-Fi networks, and how do they differ from each other?

Q.11: What is a VPN, and how can it help to establish secure Wi-Fi connections?

Q.12: What is an ad hoc network, and how does it differ from other Wi-Fi networks?

Q.13: What is the 802.11a Wi-Fi standard, and how is it different from other standards?

Q.14: What are the benefits of using the 802.11ac Wi-Fi standard?

Q.15: What is Wi-Fi 6, and how is it different from other Wi-Fi standards?

*** ***** ***