

B.Sc. III Sem
SEC-2(Information Technology)
Unit-II

1. Explain about various Security measures

Cyber Security: It is the practice of protecting computer systems, networks, and data from unauthorized access, theft, damage, or attacks by malicious actors.

Information Security: Information security programs are built around three core objectives, commonly known as the CIA (Confidentiality, Integrity, Availability):

- **Confidentiality:** Ensures information remains accessible only to authorised individuals, entities, and processes. A breach occurs when unauthorised parties gain access to sensitive data, such as passwords or personal information.
- **Integrity:** Maintains the accuracy and completeness of data by preventing unauthorised modifications. This principle ensures that only authorised personnel can edit or update information, maintaining data reliability.
- **Availability:** Guarantees that information and systems remain accessible when needed. This requires coordination between network operations, development teams, incident response, and policy management to prevent service disruptions.

Information Security Threats

There are many different risks that can harm your data and systems. Knowing about these threats helps you protect yourself better.

- **Viruses:** Viruses are self-replicating programs that attach themselves to other programs or files on host computers. They spread through infected media like songs, videos, or software downloads. Notable examples include file viruses, macro viruses, boot sector viruses, and stealth viruses.
- **Worms:** A malicious program that replicates itself to spread across systems is a **worm**. share self-replicating capabilities with viruses but operate independently without attaching to host programs. Their key distinction is network awareness—they can travel between connected computers, typically consuming system resources and slowing performance rather than causing direct damage.
- **Trojan:** Malware designed to gain unauthorized access and control of a system is called a **Trojan or Trojan horse**. The Trojan is disguised as something useful or attractive (like software, attachments, or links). When the user runs or installs it, the Trojan secretly installs malicious components. This can allow attackers to steal data, install more malware, monitor user activity, or take remote control of the computer.

Hacking: Hacking is the act of gaining unauthorized access to computer systems, networks, or digital devices by exploiting security vulnerabilities or bypassing security measures. It involves breaking into

systems without permission. Hackers may steal, modify, or destroy data. It can be done for malicious purposes (illegal hacking) or ethical reasons (ethical hacking or penetration testing).

E-mail phishing: It is a type of attack where an attacker sends deceptive emails that look legitimate in order to trick recipients into revealing sensitive information (passwords, bank details, personal data), clicking malicious links, or opening attachments that install malware. Phishing is an E-Mail threat.

2. Write about various E-Mail and its Protocols.

E-mail: An E-mail (Electronic Mail) is a method of sending and receiving messages over the Internet. It allows users to exchange text, images, documents, and other files quickly and efficiently. Each user has a unique e-mail address (like example@gmail.com) to send and receive messages.

To: The To field is where you enter the primary recipient(s) of your e-mail. These are the people directly addressed in the message, and they are expected to take action or respond.

CC (Carbon Copy): The CC field is used to send a copy of the e-mail to other recipients besides the main recipient. People in CC are usually informed about the message but are not expected to take action. All recipients can see the CC list.

BCC (Blind Carbon Copy): The BCC field is similar to CC, but recipients in BCC are hidden from others. This is used to send a copy of the e-mail without revealing the recipient's address to others in the To or CC fields.

Protocols of E-Mail:

Protocol	Full Form	Function	Usage
SMTP	Simple Mail Transfer Protocol	Sending e-mails	Outgoing mail
POP3	Post Office Protocol Version 3	Receiving & downloading e-mails	Incoming mail (single device)
IMAP	Internet Message Access Protocol	Accessing e-mails on server	Incoming mail (multi-device)
MIME	Multipurpose Internet Mail Extensions	Sending multimedia attachments	Attachments & rich content

3. Write about WWW & Related terms

WWW (World Wide Web) :The **World Wide Web** is a large collection of webpages connected through the Internet. It allows people to access information, watch videos, read articles, and much more. When you type a website address in a browser, the WWW helps display that webpage on your device. It uses protocols like HTTP or HTTPS to transfer information between computers.

Web Browser: A **web browser** is a software application that helps you open and view webpages on the Internet. Examples include Google Chrome, Mozilla Firefox, and Microsoft Edge. When you type a website address, the browser connects to the server and shows the webpage content like text, images, and videos.

ISP (Internet Service Provider): An **Internet Service Provider (ISP)** is a company that gives Internet connection to users. Without an ISP, you cannot connect to the Internet or access websites. Examples

of ISPs include BSNL, Airtel, and Jio. ISPs provide Internet through various methods like broadband, fiber, or mobile data.

Webpage: A **webpage** is a single page on the Internet that contains text, pictures, links, videos, and other content. Every webpage has a unique address called a URL. When you open a webpage in your browser, the information is loaded from a web server and displayed on your screen.

HTML (HyperText Markup Language) : HTML is the standard language used to create webpages. It gives structure to the content on the web. For example, headings, paragraphs, images, and links are all made using HTML tags. Web browsers read the HTML code and show the page in a proper layout.

Domain: A **domain** is the name or address of a website on the Internet. It is easier to remember than an IP address. For example, www.google.com is a domain name. When you type it in a browser, it takes you to the website's server. Various Domain Extensions are

Domain Extension	Full Form / Meaning	Purpose / Usage	Example
.com	Commercial	Used by businesses, companies, and commercial websites	www.amazon.com
.org	Non-Commercial Organization	Used by non-profit organizations, NGOs, and groups	www.wikipedia.org
.edu	Education	Used by educational institutions like schools, colleges, and universities	www.harvard.edu
.gov.in	Government of India	Used by Indian government websites	www.india.gov.in
.mil	Military	Used by military organizations, mainly in the USA	www.army.mil

Hosting: **Hosting** is a service that stores a website's files on a server and makes them available on the Internet. When someone visits your website, the hosting server sends the webpage to their browser. Without hosting, a website cannot be seen online.

4. Write about E-Commerce

E-Commerce (Electronic Commerce): E-commerce refers to the buying and selling of goods and services using the internet. It involves online transactions between businesses, consumers, or both, through websites, mobile apps or online marketplaces like Amazon, Flipkart and eBay.

Benefits of E-commerce:

1. Shop anytime, anywhere.
2. Products are available worldwide.

3. Saves time and travel.
4. Lower prices due to less overhead cost.
5. Easy to compare products and prices.
6. Wide variety of products available.
7. Fast and secure online payments.
8. Helps businesses reach more customers.
9. Customers can read reviews before buying.
10. Convenient home delivery of products.

5. Write about Electronic Payment Systems

Electronic Payment Systems (E-Payment Systems)

Electronic Payment System refers to a way of making financial transactions or paying for goods and services through electronic means instead of using cash or cheques. It allows people and businesses to make payments over the internet securely and quickly.

Types of Electronic Payment Systems

1. **Credit/Debit Cards:**
Payments made using cards issued by banks (like Visa, MasterCard or RuPay).
2. **Online Banking (Net Banking):**
Customers use their bank's website or app to transfer money or pay bills.
3. **Mobile Wallets:**
Apps like Google Pay, PhonePe and Paytm store money digitally for quick payments.
4. **UPI (Unified Payments Interface):**
Instant money transfer system in India using mobile numbers or UPI IDs.
5. **Electronic Fund Transfer (EFT/NEFT/RTGS/IMPS):**
Used to transfer money between bank accounts electronically.
6. **PayPal and Other Gateways:**
International online payment services for sending and receiving money globally.
7. **Smart Cards and Prepaid Cards:**
Cards that are preloaded with money and used for specific payments (e.g., metro cards).