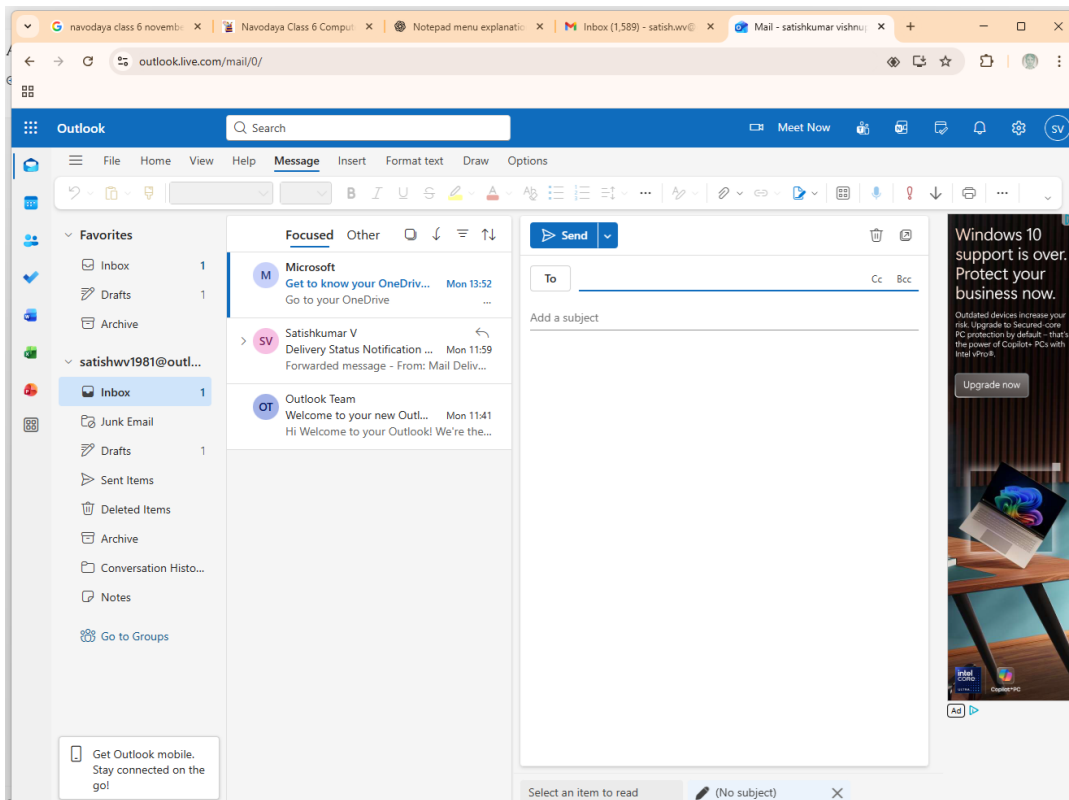
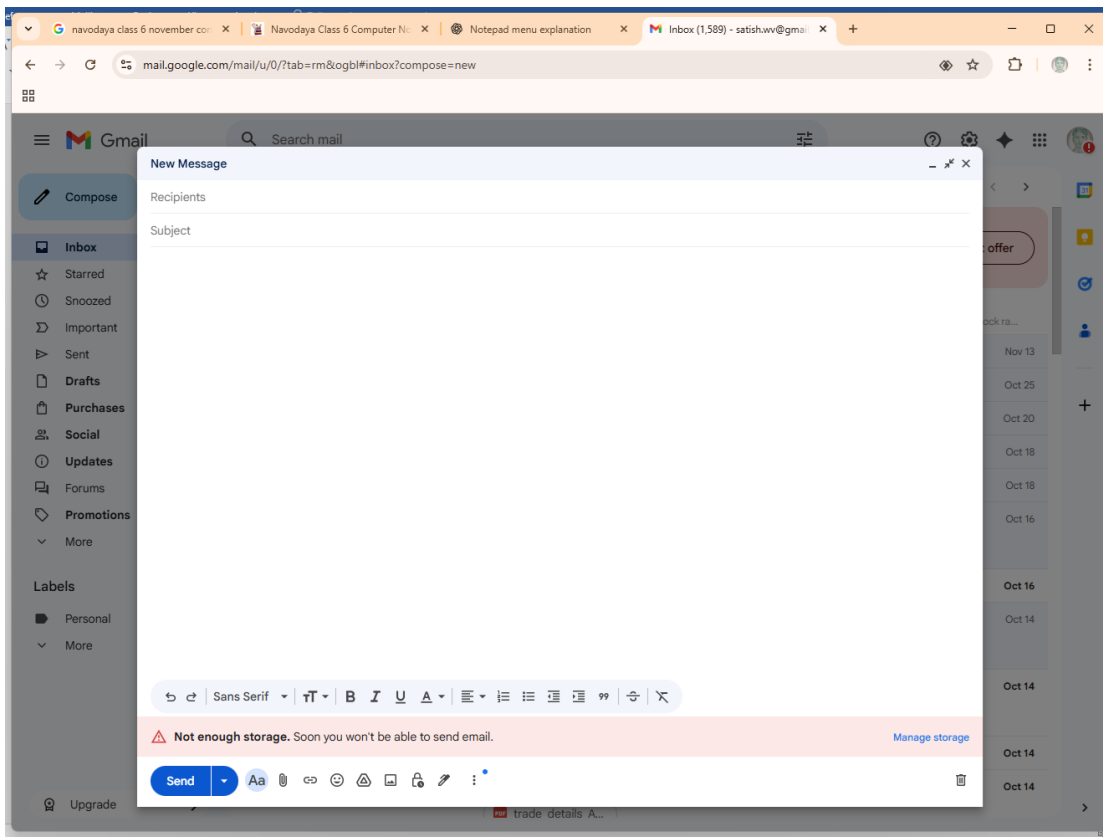


# ELECTRONIC MAIL (E-MAIL)



Email (Electronic Mail) is a method of sending and receiving messages through the Internet. It is one of the fastest and most widely used communication tools in the world.

---

## • Advantages and Disadvantages of Social Media / Social Sites

### Advantages

- Fast communication with friends, family, and people worldwide.
- Sharing information such as photos, videos, documents.
- Educational content available through pages, groups, and communities.
- Business promotion through ads and pages.
- Online meetings and collaboration through platforms.
- News and updates available instantly.

### Disadvantages

- Privacy issues – personal data may be misused.
  - Cyberbullying or online harassment.
  - Addiction leading to reduced productivity.
  - Fake news spreads quickly.
  - Security risks such as hacking or phishing.
  - Mental stress due to comparison and social pressure.
- 

## • Creating a Gmail Account

### Steps to create a Gmail account:

1. Open a browser and go to the Gmail site (mail.google.com).
  2. Click on Create account.
  3. Choose For myself or For work.
  4. Enter your details:
    - First name
    - Last name
    - Username (your email address)
    - Password
  5. Click Next.
  6. Enter phone number (for verification).
  7. Enter recovery email (optional).
  8. Set your date of birth and gender.
  9. Agree to Google's Terms and Conditions.
  10. Your Gmail account is created.
- 

## • Features of Gmail Account

- Free email service with large storage (15 GB shared with Google Drive).
  - Spam filtering automatically removes unwanted emails.
  - Labels & Filters help organize emails.
  - Search bar to quickly find emails.
  - Chat & Meet options for messaging and video calls.
  - Drafts to save unfinished emails.
  - Starred and Important sections for priority emails.
  - Sent Mail, Trash, Spam, All Mail folders.
  - Two-step verification for security.
  - Integration with Google services (Drive, Photos, Calendar, Docs, etc.).
- 

## • Compose Mail

Composing a mail means writing and sending a new email.

Steps:

1. Click Compose button.
  2. A new message window appears.
  3. Fill in the fields:
    - To: Recipient's email address
    - Subject: Title of the email
    - Message body: Main content
  4. Add attachments if required.
  5. Click Send.
- 

## • Upload & Attachment

Attachments are files you send along with your email.

Steps to attach a file:

1. In the Compose Mail window, click on the paperclip icon (Attach files).
  2. Select the file from your computer (image, document, PDF, etc.).
  3. The file uploads and appears in the email.
  4. Now send the email.
- 

## • Downloading

Downloading means saving email attachments to your device.

Steps:

1. Open the email containing the attachment.
  2. Click on the Download icon next to the attached file.
  3. The file is downloaded to your system (usually in the *Downloads* folder).
- 

- Forwarding and Reply

### Reply

Used to respond to the sender of an email.

- Open the email.
- Click Reply.
- Type your message.
- Click Send.

### Forward

Used to send the same email to another person.

- Open the email.
  - Click Forward.
  - Enter the recipient's email address.
  - Add your message (optional).
  - Click Send.
- 

- Recipient

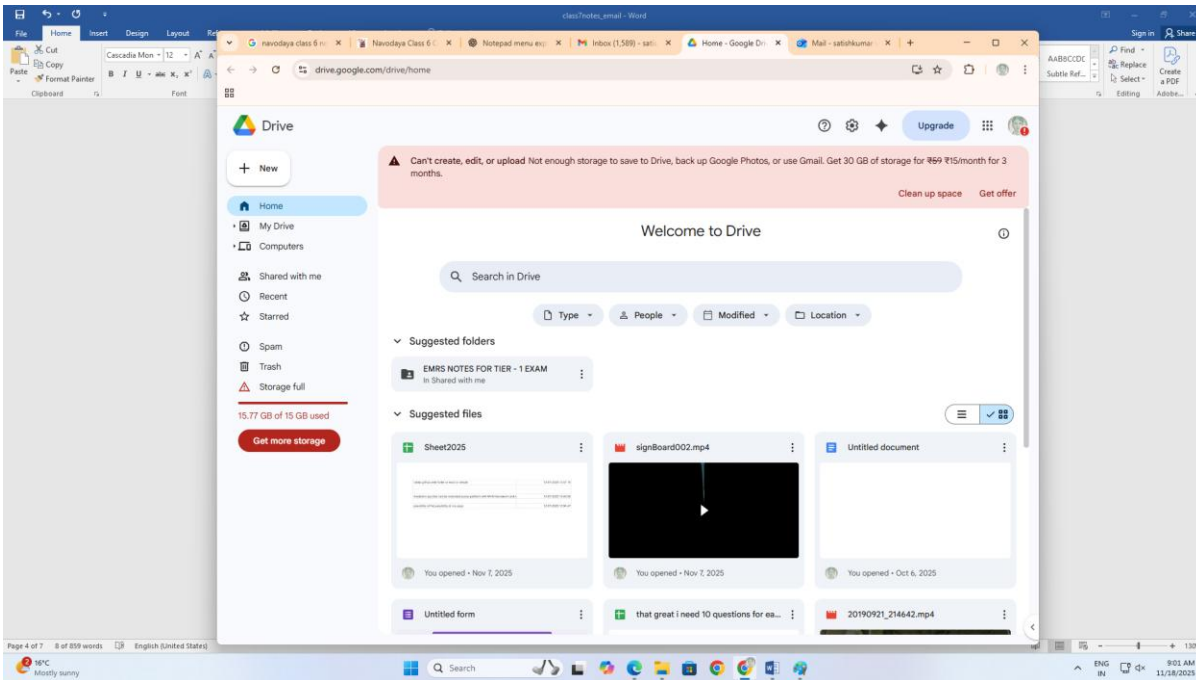
The person who receives the email.

Types:

- To: Main recipient(s).
- CC (Carbon Copy): Secondary recipients who should also see the email.
- BCC (Blind Carbon Copy): Recipients who receive the email secretly. Other recipients cannot see their addresses.

## GOOGLE DRIVE

Google Drive is a cloud storage service provided by Google. It allows users to store files online, access them from any device, share them with others, and collaborate in real-time.



---

- Create New Folder

Steps:

1. Open Google Drive (drive.google.com).
  2. Click on the New button (left side).
  3. Select Folder.
  4. Type the folder name.
  5. Click Create.
- A new folder will appear in your Drive.

---

- New File Upload

Used to upload a single file from your computer.

Steps:

1. Click New.
  2. Select File upload.
  3. Choose the file (PDF, image, document, audio, etc.).
  4. Click Open.
- The file will upload to your Google Drive.

---

- New Folder Upload

Used to upload an entire folder with multiple files.

Steps:

1. Click New.
  2. Select Folder upload.
  3. Choose the folder from your computer.
  4. Click Upload.
- Google Drive will upload all files inside that folder.
- 

- Google Sheet

Google Sheets is Google's online spreadsheet application.

Features:

- Works like Microsoft Excel.
- Used for calculations, tables, charts, and data analysis.
- Supports formulas and functions.
- Allows multiple people to work together in real time.
- Automatically saves changes in the cloud.

To create:

1. Click New.
  2. Select Google Sheets (Blank Spreadsheet).
- 

- Google Form

Google Forms is used to create:

- Surveys
- Tests
- Registration forms
- Feedback forms
- Quizzes

To create:

1. Click New.
  2. Select Google Forms.
  3. Choose Blank Form or a template.
  4. Add questions, options, images, and settings.
  5. Responses are collected automatically and can be viewed in Sheets.
- 

- How to Create a Sharable Link?

1. Right-click any file or folder in Google Drive.
  2. Click Get link.
  3. Choose access level:
    - Restricted – Only specific people can open.
    - Anyone with the link – Anyone who has the link can view/edit.
  4. Choose permission:
    - Viewer
    - Commenter
    - Editor
  5. Click Copy link.
  6. Share the link anywhere (email, WhatsApp, etc.).
- 

- Remove a File from Google Drive

Steps:

1. Right-click the file or folder.
2. Click Remove.
3. The file moves to Trash.
4. To permanently delete:
  - Go to Trash.
  - Right-click → Delete forever.

## COMPUTER SECURITY

Computer security refers to protecting computer systems, networks, and data from unauthorized access, damage, misuse, or theft. It includes techniques and tools to safeguard data confidentiality, integrity, and availability.

---

### a) Threats to Computer

Threats are possible dangers that may damage computer systems or data. Major types include:

Threat Type	Description	Examples
Virus/Malware	Programs that damage data or slow systems	File corruption, data loss
Hacking	Unauthorized access to systems	Password cracking, data theft

Threat Type	Description	Examples
Phishing	Fake emails or websites to steal information	Banking fraud emails
Spamming	Unwanted bulk messages	Ads and promotions
Trojan Horse	Malware hidden in useful software	Fake apps
Ransomware	Blocks access to system until ransom paid	Data encryption attack
Denial of Service (DoS)	Overloading servers to stop services	Server crash
Eavesdropping	Secret interception of information	Unsecured Wi-Fi attack

## b) Virus and Types

A computer virus is a malicious program that enters a computer without permission and multiplies, damaging data or system files.

### Types of Viruses

Type	Description
Boot Sector Virus	Infects boot sector of storage device
File / Program Virus	Attaches to executable files (.exe, .com)
Macro Virus	Targets macro-enabled documents (MS Word, Excel)
Polymorphic Virus	Changes its code to avoid detection
Multipartite Virus	Attacks both files and boot sector
Web Scripting Virus	Attacks through websites and browsers
Ransomware	Locks system and demands money

## c) Antivirus

Antivirus is software that detects, prevents, and removes viruses and malware.

### Examples

- Windows Defender
- Quick Heal
- McAfee
- Norton
- Kaspersky
- Avast
- Bitdefender

### Functions of Antivirus

- Scanning files and folders



- Detecting and removing malware
- Real-time protection
- Automatic updates
- Quarantine infected files

---

#### d) Software and Types of Software

Software is a set of instructions that runs computer hardware.

##### Types of Software

Category	Examples
System Software	Operating System (Windows, Linux, macOS), Device drivers, BIOS
Application Software	MS Office, Browser (Chrome), Media Player
Utility Software	Antivirus, Disk Cleanup, WinZip
Programming Software	Compilers, Interpreters, Editors
Open-source Software	Linux, LibreOffice
Customized Software	ERP, Banking Systems

---

#### e) Firewall and its Use

A Firewall is a security system that monitors and controls incoming and outgoing network traffic.

##### Uses of Firewall

- Blocks unauthorized access
- Filters harmful websites and data packets
- Protects from hackers and malware
- Protects private network from public networks (e.g., Internet)

##### Types

- Hardware firewall
  - Software firewall
- 

#### f) Cyber Crime

Cyber crime is an illegal activity performed using computers or the Internet.

## Examples

- Hacking
  - Online fraud & bank scams
  - Identity theft
  - Cyber bullying
  - Data theft
  - Ransomware attacks
  - Spreading viruses
- 

## g) Backup and Restore

### Backup

Copying data to another location so it can be recovered if lost.

#### Methods:

- Pen drive / External hard disk
- Cloud storage (Google Drive, OneDrive)
- Network backup

### Restore

Recovering lost or damaged data from backup files.

---

## h) Cyber Law and its Importance

Cyber law refers to laws that govern digital activities, electronic communication, and Internet usage.

### Importance

- Protects individuals and organizations from cyber crimes
- Defines punishment for online offenses
- Secures privacy and personal information
- Ensures safe online transactions

### Indian Cyber Law

- Information Technology Act (IT Act) 2000
- Amended in 2008 to include cyber terrorism, identity theft & privacy protection

# DETAILED LONG ANSWER QUESTIONS

---

## 1. Explain in detail the different types of threats to a computer.

Computer systems face many threats that can affect data, hardware, and overall performance.

Major threats include:

### 1. Malware

Malicious software designed to harm the system. Includes viruses, worms, trojans, ransomware, spyware, and adware.

### 2. Unauthorized Access

Hackers use cracking tools to access systems without permission and steal or modify data.

### 3. Phishing

Fake websites or emails that trick people into giving passwords, bank details, or OTPs.

### 4. Data Theft

Stealing confidential information like documents, passwords, or business data.

### 5. Hardware Threats

Power failure, overheating, dust, or physical damage can cause system failure.

### 6. Network Attacks

- DoS attacks overload servers
- Man-in-the-middle attacks intercept communication
- Packet sniffing captures data packets

### 7. Social Engineering

Attackers trick users through manipulation, pretending to be legitimate people or services.

### 8. Natural Threats

Floods, fire, storms can damage computer labs and data centers.

Impact: Data loss, financial loss, privacy issues, system breakdown.

---

## 2. What is a computer virus? Explain its characteristics and types.

A computer virus is a harmful program that attaches itself to files and spreads from one system to another. It is designed to damage data, slow performance, or gain unauthorized access.

### Characteristics of Viruses

- Replication: Can copy itself endlessly.
- Activation: Triggers when a user runs an infected file.
- Payload: Performs harmful actions like deleting files.
- Stealth: Hides itself from users or antivirus.

### Types of Viruses

#### 1. *File Infector Virus*

Infects executable files (.exe, .com). Example: Jerusalem virus.

#### 2. *Boot Sector Virus*

Attacks the master boot record, prevents system startup. Example: Michelangelo.

#### 3. *Macro Virus*

Written in macro languages like VBA, infects Word or Excel files. Example: Melissa virus.

#### 4. *Worm*

Self-replicates through networks without user action. Example: ILOVEYOU worm.

#### 5. *Trojan Horse*

Appears useful but contains hidden malicious code. Example: Fake antivirus.

#### 6. *Ransomware*

Encrypts data and asks for ransom to unlock it. Example: WannaCry attack.

## 7. Spyware

Secretly monitors and sends user activity to attackers.

## 8. Adware

Shows unwanted advertisements and slows down system.

Effects: Data corruption, slow performance, identity theft, system crash.

---

# 3. What is antivirus software? Explain its working and features.

Antivirus is a security tool that protects computers from viruses and malware.

## How Antivirus Works

1. Scanning: Checks files, RAM, and drives.
2. Detection: Uses virus signatures and heuristics to find threats.
3. Quarantine: Moves infected files to a secure area.
4. Removal: Cleans or deletes harmful software.
5. Real-time protection: Monitors system activities to block threats instantly.

## Features of Antivirus

- Full system scan
- Boot-time scan
- Automatic updates
- Email protection
- Web protection
- Ransomware protection
- Firewall integration
- Cloud-based detection

Examples: Windows Defender, Quick Heal, Avast, Kaspersky.

---

# 4. What is software? Explain its types with examples.

Software is a set of instructions that tells computers what to do. It allows hardware to function and users to perform tasks.

## 1. System Software

Controls hardware and supports the operation of the computer.

- Operating System (Windows, Linux, macOS)
- Device Drivers
- Utility Software (Disk Cleanup, Backup tools)

## 2. Application Software

Programs made for user needs.

- MS Word (document creation)
- Web browsers (Chrome, Firefox)
- Games
- Media players

## 3. Programming Software

Used for developing programs.

- Compilers (GCC)
- Interpreters (Python Interpreter)
- IDEs (VS Code, PyCharm)

Importance of Software:

- Allows communication with hardware
- Helps create documents, graphics, websites, programs
- Provides security and system management

---

## 5. What is a firewall? Describe types and uses of firewalls.

A firewall is a security system that monitors and controls network traffic. It acts as a protective barrier between the internal network and external threats.

### Types of Firewalls

1. Hardware Firewall: Physical device (in routers/switches).
2. Software Firewall: Installed on operating systems (Windows Firewall).
3. Packet Filtering Firewall: Filters data packets based on rules.
4. Proxy Firewall: Hides internal network by acting as an intermediary.
5. Next-Gen Firewall: Includes deep packet inspection, intrusion prevention.

### Uses

- Blocks unauthorized access

- Protects against hacking and malware
  - Monitors incoming and outgoing traffic
  - Filters harmful or blocked websites
  - Prevents data leakage
- 

## 6. Explain cybercrime in detail. What are its major types?

Cybercrime is criminal activity performed through computers or the internet. Attackers misuse technology to harm people, steal data, or damage systems.

### Major Types of Cybercrime

1. Hacking: Breaking into systems.
2. Phishing: Fake messages asking for passwords.
3. Identity Theft: Stealing personal information.
4. Online Fraud: Fake shopping websites, lottery scams.
5. Ransomware Attacks: Locking data for ransom.
6. Cyberbullying: Online harassment or threats.
7. Spreading Malware: Creating or distributing harmful software.
8. Data Breach: Accessing confidential information.
9. Cyber Terrorism: Attacks on national security systems.

### Effects

- Financial loss
  - Privacy loss
  - System damage
  - Psychological harm
  - National security threats
- 

## 7. Explain backup and restore. Why are they important for computer safety?

Backup and Restore are essential processes to protect data.

### Backup

Creating a secondary copy of important data.

#### Types of backup:

- Full backup
- Incremental backup
- Differential backup

- Cloud backup
- External storage backup

Reasons for backup:

- Viruses and ransomware
- Hard disk crash
- Accidental deletion
- Natural disasters
- System formatting

Restore

Recovering lost or damaged data from backup.

Importance:

- Ensures business continuity
- Saves time and effort
- Protects against huge data loss
- Provides disaster recovery

## 8. What is cyber law? Explain its importance and components.

Cyber law consists of laws that govern digital activities, internet use, and online crimes.

Importance of Cyber Law

- Protects users from cyber fraud
- Controls misuse of electronic data
- Provides guidelines for digital transactions
- Ensures privacy and data protection
- Helps punish cybercriminals
- Supports safe e-governance, e-commerce

Main Components

1. IT Act 2000 (India): Deals with electronic records, digital signatures, cybercrime laws.
2. Intellectual Property Rights: Protects software, digital content.
3. Data Protection Laws: Protect personal information.
4. Cyber Forensics: Helps investigate online crimes.

Cyber laws create a safer digital environment for individuals, businesses, and government.