Studybeesofficial

Where Minds Pollinate

Class 12
Computer

Chapter 6

Impact of computing notes

Follow Our Socials

studybeesofficial
studybeesofficialpak
studybeesofficialpak

Chapter 6 # Impact of Computing

Introduction

- The digital world requires **cyber safety practices** for online collaboration.
- **Key goals:**
  - Protect participant **privacy**.
  - Ensure **equal access** to information for everyone, regardless of background.
- **Essential techniques mentioned:**
  - Two-factor authentication
  - Biometric verification
  - Secure data transmission

6.1 Security Protocols

- **Definition:** Rules and procedures to protect data from unauthorized access, tampering, and interception.
- **Purpose:** Essential for data protection, risk management, regulatory compliance, and building trust.

6.1.1 Need of Security Protocols

Security protocols are crucial for several reasons:

1. **Confidentiality**
   - Keeps data secret and accessible only to authorized parties.
   - **Primary Technique: Encryption** - converts data into a format that can only be read with a decryption key.
2. **Data Integrity**
   - Ensures information remains **accurate, consistent, and unaltered** during storage, transmission, and processing.
   - Security protocols prevent unauthorized changes or fraud.
3. **Authentication**
   - Verifies the identity of a user or device.
   - Ensures only authorized people/systems can access or send data.
   - **Common Techniques:** Usernames/passwords, multi-factor authentication (MFA), digital certificates.

4. **Access Control**
    - Mechanisms that decide **who can access, change, or send data**.
    - Protects information and privacy by preventing unauthorized access or misuse.
5. **Secure Transmission**
    - Protects data while it is being sent over networks.
    - **Tools:**
        - **SSL/TLS:** Used for securing website connections.
        - **VPNs (Virtual Private Networks):** Used for secure remote connections.
    - These tools encrypt data during transmission, making it unreadable to interceptors.
6. **Protection Against Malware and Cyberattacks**
    - Help defend against viruses, malware, and other cyber threats.
    - **Examples of Security Measures:** Firewalls and anti-malware tools, which operate based on established protocols.
7. **Data Backup and Recovery**
    - Ensure data can be recovered if lost due to failure, loss, or a cyberattack.
    - Involves **regular backups** and **secure storage rules**.

6.1.2 Information Usage and Collection

- **Core Principles:** Transparency, Permission, and Legality.
- Organizations must:
    - Clearly state why data is being collected.
    - Obtain consent where necessary.
    - Protect the data effectively.
    - Failure to do so can lead to legal issues and loss of trust.
- **Collection:**
    - The process of gathering information from various sources.
    - **Methods:** Surveys, interviews, sensors, software.
    - **Data Forms:** Numbers, text, images.

- **Usage:**
    - **Key Purposes:**
        - Offer and improve services/products.
        - Personalize content.
        - Perform analytics.
    - **Specific Examples:**
        - Understand customer preferences.
        - Track student performance to enhance learning.
        - Monitor patient health for treatment development.
        - Train AI models or enhance apps and systems.

6.2 Risks of Sharing Private Information

The primary risk is **Identity Theft** - when someone uses your personal details without permission for fraud, leading to financial loss and reputational damage.

A **scammer** is a **person or group** who tries to **cheat or deceive others**—usually to **steal money, personal information, or valuables**—by using **lies, tricks, or fake identities**.

How Identity Thieves Get Information:

1. **Phishing:**
    - Scammers send fraudulent emails, texts, or messages pretending to be from trusted organizations.
    - Goal: Trick you into providing passwords or financial details.
2. **Data Breaches:**
    - When organizations are hacked, customer data can be stolen and exposed.
    - Your data is at risk if you are a customer of a breached company.
3. **Lost or Stolen Items:**
    - Physical items like wallets, laptops, or documents containing personal info can be lost or stolen and then misused.
4. **Online Scams:**

- Scammers create fake websites or ads to fool people into giving away personal information or money.

6.3 Best Practices to Prevent Identity Theft

- **Be Cautious Sharing Info:** Be careful when asked for personal info via email, phone, or social media.
- **Use Strong Passwords:** Create strong, unique passwords for all online accounts.
- **Use a Password Manager:** Helps to keep track of multiple complex passwords.
- **Enable Multi-Factor Authentication (MFA):** Adds an extra layer of security beyond just a password.
- **Monitor Financial Statements:** Regularly check bank and credit card statements for any unusual activity.
- **Check Credit Reports:** Review your credit reports regularly for signs of fraudulent accounts.
- **Protect Physical Items:** Secure IDs, passports, and credit cards.
- **Stay Informed:** Learn about common scams and be cautious online.

Cyber Attack

A **cyber attack** is a **malicious attempt to damage, disrupt, or gain unauthorized access** to computer systems, networks, or data.

It targets both individuals and organizations, threatening **security, privacy, and operations**.

Types of Cyber Attacks:

1. Virus

Definition: A malicious program that attaches to legitimate files and spreads when those files are executed.

Examples:

1. **Melissa Virus (1999):** Spread through infected Word documents via email attachments.
2. **MyDoom Virus (2004):** One of the fastest-spreading email worms; disrupted global internet traffic.

2. Spyware

Definition: Software that secretly monitors and collects user activity or personal data without permission.

How Spyware Works?

Spyware sneaks into a computer or phone through:

- Fake software downloads
- Clicking unknown links
- Opening infected email attachments
- Free apps that contain hidden malicious code

Examples:

1. **Pegasus Spyware:** Used to spy on journalists, and officials by infecting smartphones.
2. **CoolWebSearch:** Redirected users to unwanted sites and collected browsing data.
3. **FinSpy:** Used for government surveillance, allowing remote access to devices and communications.

3. Adware

Definition: Unwanted software that automatically displays or downloads advertising material when a user is online.

Examples:

1. **Fireball (2017):** Chinese adware that took control of browsers on 250 million computers.
2. **Gator (Gain Adware):** Displayed pop-up ads and tracked browsing behavior.
3. **DeskAd (2000s):** Injected banner ads into web pages and slowed system performance.

4. Malware (Malicious Software)

Definition: Any software intentionally designed to harm or exploit systems.

Examples:

1. **WannaCry Ransomware (2017):** Encrypted files worldwide, demanding Bitcoin ransom.
2. **NotPetya (2017):** Disguised as ransomware but designed to destroy data.

5. Phishing

Definition:
Phishing is a cyberattack where attackers trick users into revealing personal or

confidential information (like passwords, credit card numbers, or login details) by pretending to be a trustworthy source — such as a bank, company, or government agency.

How it Works:

- The attacker sends a fake email, message, or link that looks legitimate.
- The victim clicks the link and enters sensitive data into a fake website.
- Attackers then steal or misuse this information.

Real-World Examples:

1. **Google & Facebook (2013–2015):** A Lithuanian hacker tricked employees with fake invoices, stealing over $100 million.
2. **PayPal Phishing Scam:** Fake PayPal emails asked users to "verify their account," leading them to a fraudulent login page.
3. **COVID-19 Vaccine Phishing (2021):** Fake health department emails lured victims to malicious websites pretending to offer vaccine appointments.

6. DDoS (Distributed Denial of Service) Attack

Definition:
A DDoS attack floods a server, website, or network with excessive traffic from multiple sources, making it slow or completely unavailable to legitimate users.

How it Works:

- Attackers control thousands of infected devices (a "botnet").
- These devices send massive data requests to a target server.
- The system crashes or becomes too overloaded to function.

Real-World Examples:

1. **GitHub Attack (2018):** Suffered one of the largest DDoS attacks at 1.35 terabits per second, temporarily taking the site offline.
2. **Dyn DNS Attack (2016):** A massive DDoS attack disrupted Twitter, Netflix, Amazon, and Spotify services.
3. **New Zealand Stock Exchange (2020):** Trading halted for several days after repeated DDoS attacks on its network.

7. Ransomware

Definition:
Ransomware is a type of malicious software that encrypts a user's files or system, locking access until the victim pays a ransom (usually in cryptocurrency) to the attacker.

How it Works:

- Malware enters via email attachments, links, or vulnerabilities.
- It encrypts data on the system.
- The attacker demands payment to provide a decryption key.

Real-World Examples:

1. **WannaCry (2017):** Spread globally across 150 countries, encrypting data and demanding Bitcoin ransom from hospitals, businesses, and governments.
2. **NotPetya (2017):** Initially disguised as ransomware but designed to destroy data; heavily impacted Ukraine and multinational companies.
3. **Colonial Pipeline Attack (2021):** Ransomware disrupted U.S. fuel supply; company paid $4.4 million to regain control.

8. Human Error

Definition: Mistakes by individuals that lead to data breaches or system compromise.

Examples:

1. **Target Data Breach (2013):** Employees clicked phishing emails leading to stolen credit card data.
2. **British Airways (2018):** Misconfigured website led to theft of customer payment data.
3. **NASA Data Loss (2018):** Employee's stolen laptop contained unencrypted sensitive information.

9. Software Failure / Error

Definition: Security vulnerabilities or bugs in software that attackers exploit.

Examples:

1. **Equifax Breach (2017):** Attackers exploited a flaw in Apache Struts software.
2. **Heartbleed Bug (2014):** Flaw in OpenSSL exposed private data across the internet.
3. **Microsoft Exchange Hack (2021):** Hackers exploited zero-day vulnerabilities in mail servers.

Threat	Definition	How It Works	Example
DDoS Attack (Distributed Denial of Service)	A cyberattack where multiple compromised computers flood a target server or website with	Attackers infect many computers (a botnet), then command them to send huge amounts of requests to the target. The server becomes	**GitHub DDoS Attack (2018) –** one of the largest DDoS attacks recorded (1.35 Tbps).

	excessive traffic, causing it to slow down or crash.	overloaded and unavailable to normal users.	
Ransomware	Malicious software that encrypts files and demands payment (ransom) to unlock them.	Enters through infected emails, downloads, or vulnerabilities. Once inside, it encrypts important files and displays a ransom message. Victims must pay in cryptocurrency to get a decryption key.	**WannaCry (2017)** – infected 200,000+ computers worldwide using EternalBlue exploit.
Spyware	Malware that secretly monitors and collects user information without permission.	Installs silently; runs in background; records keystrokes, browsing habits, screenshots, passwords, and sends them to the attacker.	**Keyloggers** that record everything a user types (passwords, messages).
Virus	Malicious program that attaches itself to legitimate files and spreads when the infected file is run.	Needs human action to spread (opening files, sharing USBs). Once activated, it corrupts files, slows systems, or causes data loss.	**MyDoom Virus (2004):** One of the fastest-spreading email worms; disrupted global internet traffic.
Phishing	A social engineering attack where attackers trick users into giving personal data (passwords, banking info) through fake emails or websites.	Attackers send fake emails that look real (often using spoofing). Users click the link and enter their credentials into a fake website controlled by criminals.	Fake "**Your bank account is locked** — verify now" emails.
Malware	Any software intentionally designed to cause harm to a computer system. It includes viruses, worms, ransomware, spyware, trojans, etc.	Enters through downloads, malicious websites, infected USBs, phishing emails, or software vulnerabilities. Once inside, it damages files, steals data, or controls the system.	**Trojan Horse malware** disguised as a free game or software download.

Security Methods:

Security methods are the **techniques and technologies used to protect systems, data, and user identities** from unauthorized access, misuse, or attacks.
They form the foundation of **cybersecurity**, ensuring **confidentiality, integrity, and availability** of information.

1. Two-Factor Authentication (2FA)

Definition:
2FA adds an extra layer of security by requiring **two types of verification** before granting access — usually something you *know* (password) and something you *have* (phone, OTP).

Example:

- Logging into Gmail requires a password (factor 1) and a one-time code sent to your mobile (factor 2).
- Even if a hacker steals your password, they still can't log in without the code.

Purpose:

- Prevents unauthorized access due to stolen passwords.
- Commonly used in email, banking, and cloud services.

Biometric Verification

Definition:
Uses **unique physical or behavioral traits** (like fingerprints, facial features, voice, or iris patterns) to verify identity.

Example:

- Unlocking a smartphone using **fingerprint** or **face recognition**.
- Airport immigration gates using **iris scanners**.

Purpose:

- Hard to fake or steal compared to passwords.
- Provides quick and secure authentication.

Password Protection

Definition:
Using strong, unique passwords and managing them securely.

Example:

- Using complex combinations (uppercase, lowercase, numbers, symbols).
- Regularly updating passwords and avoiding reuse.

Purpose:

- First line of defense against unauthorized access.
- Weak passwords are a leading cause of breaches.

Security Method	How It Works	Purpose	Example
2FA	Uses password + secondary code	Prevents unauthorized login	Gmail OTP
Biometric Verification	Uses fingerprint/face recognition	Confirms true identity	Smartphone unlock
Encryption	Converts data into unreadable form	Protects data privacy	WhatsApp messages
Firewalls	Filters network traffic	Blocks suspicious access	Company network security
Antivirus	Scans and removes malware	Prevents infection	Norton, Windows Defender
Access Control	Role-based permissions	Restricts data exposure	Admin vs. user roles

Cipher Methods in Cryptography:

A **cipher** is a method of **encrypting (encoding)** text so that it becomes unreadable to unauthorized people.
The process of turning readable text (**plaintext**) into coded text (**ciphertext**) is called **encryption**, and turning it back is called **decryption**.

1. Caesar Cipher

One of the simplest and oldest encryption techniques.
Each letter in the plaintext is **shifted by a fixed number of positions** in the alphabet.

Example (Shift by 3):
Plaintext: HELLO
Shift each letter by +3 →
H → K, E → H, L → O, L → O, O → R

Ciphertext: KHOOR

Decryption:
Shift letters **back by 3** to get the original message.

Used by: Julius Caesar for military communication.

Plaintext	Ciphertext	Explanation
HELLO	**KHOOR**	H→K, E→H, L→O, O→R
CAT	**FDW**	C→F, A→D, T→W
SCHOOL	**VFKRRO**	S→V, C→F, H→K, O→R, O→R, L→O
PYTHON	**SBWKRQ**	P→S, Y→B, T→W, H→K, O→R, N→Q

2. Substitution Cipher

Each letter in the plaintext is **replaced by another letter or symbol**, but not necessarily in a simple sequence like Caesar's.
It uses a **mapping rule or key alphabet**.

Example:

Atbash Cipher (Reverse Alphabet Cipher)

- Reverses the alphabet — A ↔ Z, B ↔ Y, C ↔ X, etc.
- It's still substitution, but with a fixed **reverse rule**, not a numeric shift.

Example:
Plaintext: HELLO
H → S, E → V, L → O, L → O, O → L
Ciphertext: SVOOL

Decryption: Reverse again (S→H, V→E, etc.)

Notice: No shifting; it's a **letter-to-letter mapping based on position**.

Plaintext Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher Alphabet	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Plaintext	Ciphertext	Explanation
HELLO	**SVOOL**	H→S, E→V, L→O, O→L
COMPUTER	**XLNKFGVI**	C→X, O→L, M→N, P→K, U→F, T→G, E→V, R→I
DATA	**WZGZ**	D→W, A→Z, T→G, A→Z
SECURITY	**HVXFIRGB**	S→H, E→V, C→X, U→F, R→I, I→R, T→G, Y→B

3. Transposition Cipher

Unlike substitution (which changes letters), transposition **rearranges the positions of letters** according to a pattern or key.
The letters remain the same — only their **order changes**.

Example:
Plaintext: HELLO WORLD
Remove spaces → HELLOWORLD
Use a key that rearranges letters in groups of 5 (e.g., reverse each group):

HELLO → OLLEH
WORLD → DLROW

Ciphertext: OLLEHDLROW

Decryption:
Reverse the order again to get back HELLOWORLD.

Key Idea:
No letter substitution — only **position rearrangement**.

Plaintext	Ciphertext	Explanation
HELLO	**OLLEH**	Reverse all letters
COMPUTER	**RETUPMROC**	Reverse entire word
INFORMATION	**NOITAMROFNI**	Reverse order of letters
SECRET DATA	**TERCES ATAD**	Reverse each word separately

4. Vigenere Cipher

A more advanced **polyalphabetic cipher**, meaning it uses **multiple Caesar ciphers** with different shift values based on a **keyword**.

Example:
Plaintext: HELLO
Keyword: KEY
(Repeat keyword to match length → KEYKE)

Plaintext H E L L O

Keyword K E Y K E

Ciphertext: RIJVS

Decryption:
Subtract the same keyword shifts.

Key Advantage:
Harder to crack than simple Caesar because each letter uses a **different shift**.

Plaintext	Keyword	Ciphertext	Explanation
HELLO	KEYKE	**RIJVS**	H(+10)→R, E(+4)→I, L(+24)→J, L(+10)→V, O(+4)→S
DATA	KEYK	**NEBQ**	D(+10)→N, A(+4)→E, T(+24)→B, A(+10)→Q
SECURITY	KEYKEYKE	**CIOIWQXC**	Each letter shifted according to keyword
COMPUTER	KEYKEYKE	**MSAQCIBB**	Same pattern; multiple Caesar shifts applied

Security Protocols:

Security protocols are **rules and procedures that ensure safe communication** between computers over a network (especially the Internet).
They protect **data privacy, integrity, and authenticity** during transmission.

Think of them as **digital safety guards** that make sure:

- No one can **read** your data (Confidentiality),
- No one can **change** your data (Integrity),
- You are **talking to the right person/system** (Authentication).

Why We Need Security Protocols

Without security protocols:

- Hackers could **intercept** or **alter** your online messages.
- Passwords and personal data could be **stolen** during transfer.
- Fake websites could **pretend to be real** (e.g., fake banking sites).

Types of Security Protocols:

1. SSL / TLS (Secure Sockets Layer / Transport Layer Security)

To **secure communication between web browsers and web servers** — i.e., to protect websites and online transactions.

How It Works:

- Encrypts the data (so others can't read it).
- Authenticates the website using a **digital certificate**.
- Ensures data is not changed during transfer.

Example:
When you visit a secure website starting with https://, TLS/SSL keeps your data (like login or bank info) private.
The lock icon in the browser means **TLS/SSL** is active.

Difference:

- SSL = older version (no longer used).
- TLS = newer, more secure version.

2. IPsec (Internet Protocol Security)

Purpose:
To secure **data at the network layer** (the level below websites and apps).
It's used mainly in **Virtual Private Networks (VPNs)**.

How It Works:

- Encrypts and authenticates all data packets sent between two devices.
- Protects all Internet traffic — not just websites.

Example:
When you connect to your school or office VPN, IPsec ensures all your network data travels securely through the Internet.

Aspect	VPN (Secure Use)	VPN (Misuse / Illegal Use)
Purpose	Protects privacy, secures data	Bypasses laws or restrictions

Example Use	Securely connect to office or university network	Access banned sites or spread malware
Data Encryption	Yes, keeps information private	Yes, but used for hiding malicious actions
Legality	Legal in most countries	Illegal when used for crime or policy violation
Control	Used ethically by individuals and organizations	Misused by hackers or cybercriminals

- **AH (Authentication Header)** → proves your data is real
- **ESP** → hides (encrypts) your data
- **SA** → agreement on how to secure the data
- **Transport mode** → protects data only
- **Tunnel mode** → protects entire packet (best for VPN)

3. SSH (Secure Shell)

Purpose:
To securely **log in and control remote computers** over a network.

How It Works:

- Encrypts all commands and data sent between your computer and a remote system.
- Prevents eavesdropping and password theft.
- Commonly used by system administrators or developers.

Example:
A college IT technician uses SSH to safely access and manage servers in another city.

4. SFTP (Secure File Transfer Protocol)

Purpose:
To securely **transfer files** between computers over a network.

How It Works:

- Uses the **SSH protocol** for encryption and authentication.
- Ensures files are not intercepted or altered during upload/download.

Example:
Teachers upload exam data securely to a school's central server using SFTP instead of normal FTP.

FTP = unsecure (plain text)
SFTP = secure (encrypted)

5. HTTPS (HyperText Transfer Protocol Secure)

Purpose:
To securely **access and share data on websites** — it's the secure version of HTTP.

How It Works:

- Combines **HTTP + TLS/SSL**.
- Encrypts all communication between your web browser and the website.
- Prevents hackers from stealing personal or banking information.

Example:
When you shop online (https://amazon.com), HTTPS ensures your payment details are safe.

Visual clue:
Lock symbol + "https://" in the address bar.

Protocol	Full Form	Main Use	How It Secures Data	Example
SSL / TLS	Secure Sockets Layer / Transport Layer Security	Secure web connections	Encrypts data between browser & server	Banking, emails
IPsec	Internet Protocol Security	Network-level protection	Encrypts all IP packets	VPNs
SSH	Secure Shell	Remote login to computers	Encrypts login & commands	Server management
SFTP	Secure File Transfer Protocol	File transfers	Encrypts files using SSH	Uploading confidential files
HTTPS	HyperText Transfer Protocol Secure	Secure websites	Encrypts web pages with TLS	Online shopping, forms

Troubleshooting Security Problems:

Troubleshooting security problems means **finding, analyzing, and fixing issues that put data or systems at risk** — such as hacking attempts, malware infections, or unauthorized access.

The goal is to **detect the problem early**, **prevent damage**, and **strengthen security** to avoid future attacks.

Step	Action	Explanation (Simple Terms)
1. Identify the Issue	Detect unusual activity or alerts.	Observe signs like slow performance, unauthorized access, or suspicious messages. Example: sudden password change alerts.
2. Understand the Environment	Study the affected system or network.	Find out what devices, users, and data are involved so you can understand where the threat came from.
3. Access Control and Permissions	Check user permissions and access rights.	Make sure only authorized users can access sensitive information. Revoke access for unknown or inactive accounts.
4. User Education	Train users on safe practices.	Teach staff or students about phishing emails, strong passwords, and avoiding unsafe downloads. Human error often causes security breaches.
5. Regular Backups	Maintain copies of important data.	If an attack (like ransomware) damages files, backups help restore lost data safely.
6. Document and Learn	Record what happened and what was done.	Keep notes about the issue, solutions, and prevention methods for future reference.
7. Regular Testing and Assessment	Test security systems regularly.	Use tools like antivirus scans, firewalls, and vulnerability tests to check system strength and fix weak points.

Example Scenario

Problem: A college network detects repeated login failures and unauthorized access to staff files.

Troubleshooting Steps:

1. Identify the issue — find the unauthorized login attempts.
2. Understand environment — check which system or account was targeted.
3. Access control — reset passwords, remove old user accounts.
4. Educate users — train staff to use stronger passwords.
5. Backups — restore affected data if anything was tampered with.
6. Document — note the attack details and system response.
7. Test — run a vulnerability scan to confirm the issue is fixed.

Identifying a Cybersecurity Threat:

Identifying cybersecurity threats means **detecting possible dangers** that could harm computers, networks, or data — such as malware, phishing, data breaches, or unauthorized access — **before** they cause damage.

Various Strategies to Identify Cybersecurity Threats:

Strategy	Explanation (Simple Terms)	How It Helps Identify Threats	Example
1. Employee Training and Awareness	Teaching users how to recognize suspicious emails, links, or software.	Users become the first line of defense — they can spot phishing emails, strange pop-ups, or data leaks early.	Conducting monthly security awareness sessions at school or office.
2. Email Filtering	Automatically scans and sorts incoming emails for spam or phishing.	Detects suspicious attachments, fake sender addresses, or harmful links before they reach users.	Gmail or Outlook moves dangerous messages to the spam folder.
3. Anti-Phishing Software	Detects and blocks websites or messages that try to steal passwords or data.	Warns users if they are about to visit a fake or malicious website.	Chrome shows “Deceptive site ahead” for scam websites.
4. Secure Communication Protocols (e.g., HTTPS, TLS, SSH)	Encrypt data while it travels between computers and servers.	It prevents attackers from spying on or tampering with sensitive information.	Websites with “https://” ensure secure login and payment data transfer.
5. Web Content Filtering	Controls and restrictions on which websites users can access.	Blocks malicious or suspicious websites that may spread malware or collect data illegally.	School or office network blocks harmful websites automatically.
6. Security Updates and Patch Management	Regularly installing software updates and patches from trusted vendors.	Fixes known security weaknesses before hackers exploit them.	Windows Update or antivirus updates patch system vulnerabilities.

Computing Application:

Importance of Collaboration:

1. Diverse Perspective
People from different backgrounds, skills, and cultures bring new ideas and identify issues others might miss.

2. Enhanced Innovation
Collaboration leads to creativity — brainstorming multiple solutions before coding improves innovation.

3. Resource-Centered Design

Applications should be designed around **available resources** (hardware, internet, user devices) and user needs

4. Resource Sharing
Collaborators share computing power, cloud storage, and code libraries to complete projects faster.

5. Problem Solving
Collaboration helps teams identify, analyze, and solve complex computing problems.

Resources for Equal Information Accessibility:

Digital Libraries
Online libraries (like National Digital Library of Pakistan) provide free access to books, journals, and multimedia.

Accessible Learning Platforms
E-learning tools should support students with different abilities — e.g., text-to-speech, captions, high contrast, screen readers.

Community Information Centers
Public centers where citizens access computers and the internet for education, job applications, or e-services.

Mobile Applications
Mobile apps make information accessible to people without computers (e.g., WhatsApp learning groups, e-gov apps).

Open Educational Resources (OER)
Free online learning materials — like Khan Academy or OpenStax — allow anyone to learn without cost.

Digital Literacy
The ability to use computers, the internet, and digital tools safely and effectively.

Partnerships and Collaborations
Schools, governments, and companies can work together to provide better digital access for everyone.

Tool	Main Use	Key Features	Example in School
Google Drive	File storage and collaboration	Real-time editing, sharing, cloud storage	Group report writing in Docs
Slack	Team communication	Channels, file sharing, app integrations	Discussion channels for projects
Trello	Project management	Task boards, checklists, deadlines	Assigning and tracking project work
Microsoft Teams	Unified collaboration	Chat, meetings, file sharing	Virtual classroom with shared files
Zoom	Video conferencing	Meetings, screen share, record	Online class or group meeting