6 Impacts of Computing

Learning Outcomes

At the end of this unit students will be able to:

- Identify and apply safe practices when collaborating on digital or online platforms.
- Discuss security threats and mitigation such as 2FA, biometric verification, and secure techniques for transmitting data etc
- Collaborate on strategies to provide equity and equal access to information

Introduction

In today's digital world, using online platforms for collaboration requires awareness of cyber safety practices. It is crucial to identify and apply security measures to protect participants' privacy. Techniques like two-factor authentication, biometric verification, and secure data transmission are essential. Ensuring everyone has equal access to information, regardless of their background, is also important. By working together on these strategies, we can create a safer and more inclusive online environment for all.

6.1 Security Protocols

Security protocols are vital for protecting data in today's digital world. They set rules and procedures to prevent unauthorized access and tampering. These protocols ensure confidentiality through encryption, maintain data integrity and verify user identity with authentication methods. They also control access, secure data transmission, and ensure compliance with regulations. Additionally, they protect against malware, support data backup and recovery, reduce risks, and build trust. Security protocols are essential for data protection, risk management, and regulatory compliance.

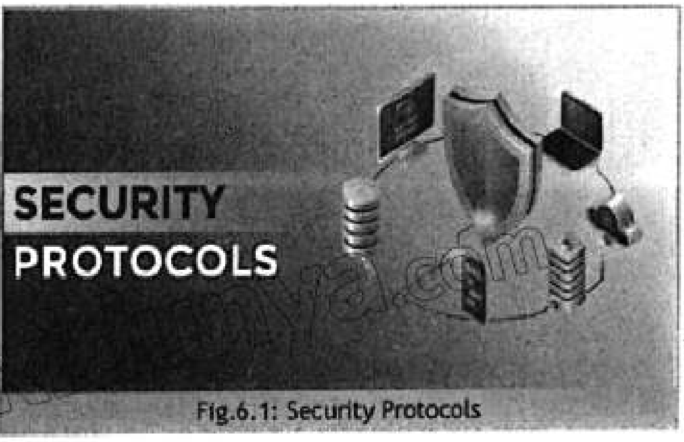
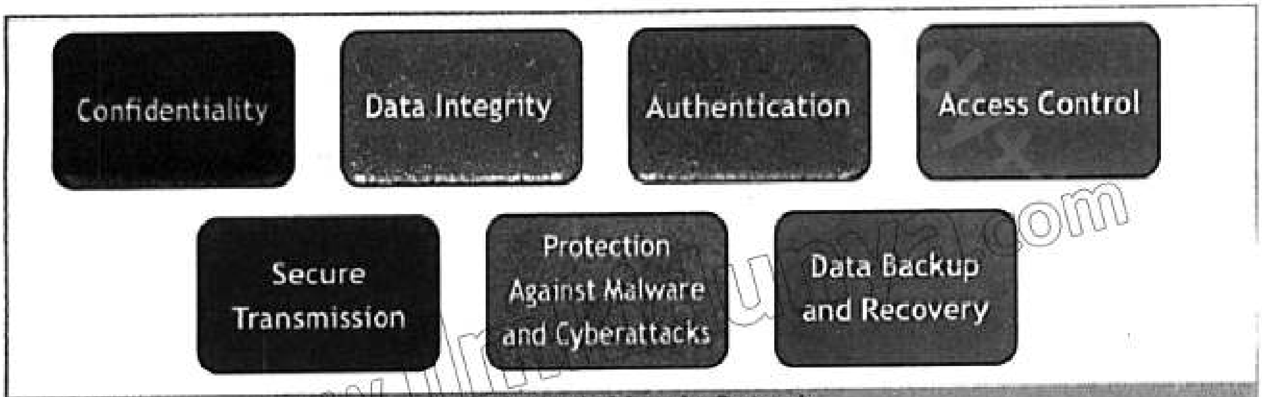


Fig.6.1: Security Protocols

6.1.1 Need of Security Protocols:

Security protocols are crucial for keeping data safe in today's digital world. They create rules and procedures to protect data from unauthorized access, tampering, and interception. Here are some key reasons why security protocols are important for data protection.



Confidentiality

Data Integrity

Authentication

Access Control

Secure Transmission

Protection Against Malware and Cyberattacks

Data Backup and Recovery

Fig.6.2: Need of Security Protocols

Confidentiality:

Security protocols, like encryption, keep data confidential. Encryption changes data into a format only accessible by authorized parties with decryption keys. This stops unauthorized individuals from accessing sensitive information.

Data Integrity:

Data integrity ensures that information remains accurate, consistent, and unaltered during storage, transmission, and processing. Security protocols like encryption protect data integrity by preventing unauthorized changes or fraud.

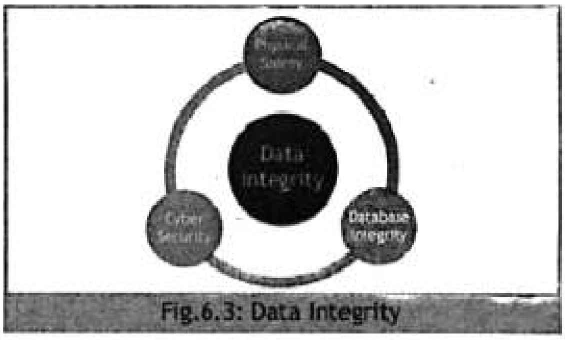


Fig.6.3: Data Integrity

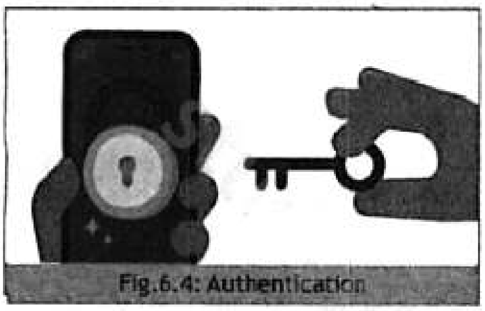


Fig.6.4: Authentication

Authentication:

Security protocols use authentication to verify user or device identities. This ensures that only authorized people or systems access or send data. Common techniques include usernames and passwords, multi-factor authentication, and digital certificates an electronic document used to prove ownership.

Access Control:

Security protocols enable access control mechanisms. These controls decide who can access, change, or send data. It ensures only authorized users access data, systems, and places. It is done through various methods to protect information and privacy, preventing unauthorized access or misuse.

Fig.6.5: Access Control

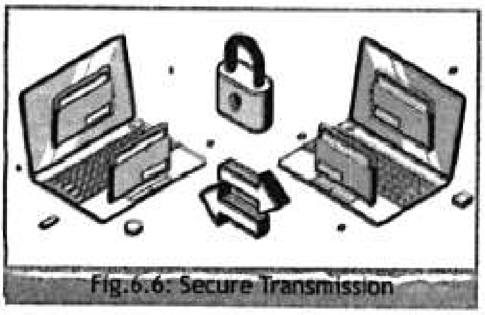


Fig.6.6: Secure Transmission

Secure Transmission:

Sending data online can be risky because hackers might try to spy. However, tools like SSL (Secure Sockets Layer)/TLS (Transport Layer Security) for websites and VPNs (Virtual private networks) for remote connections encrypt your data, making it like a secret code that only you and the intended recipient can understand. This way, even if hackers try to listen, they cannot make sense of the information.

Protection Against Malware and Cyberattacks:

Security protocols help protect against malware, viruses, and cyberattacks. Security protocols are guard against malware and cyberattacks. Firewalls and anti-malware tools are examples of security measures that rely on protocols to function effectively.

Fig.6.7: Protection Against Malware and Cyberattacks

Data Backup and Recovery:

Data security protocols cover backup and recovery. Regular backups and secure storage rules make sure data can be brought back if it's lost, hardware failure, or there is a cyberattack.

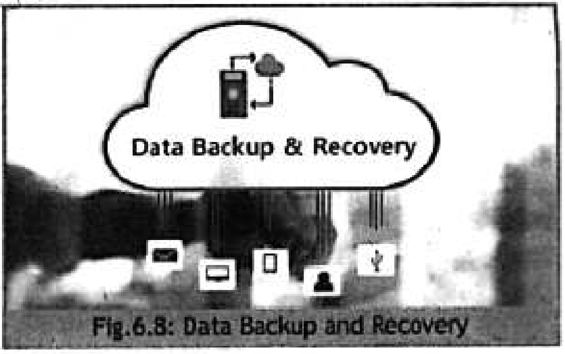


Fig.6.8: Data Backup and Recovery

6.1.2 Information usage and collection:

The main rules for collecting and using data are being clear, getting permission, and following the law. Organizations should explain why they collect data, ask for permission when needed, and protect data well. Breaking these rules can lead to big problems, legally and in how much people trust them.

Fig.6.9: Information usage and collection

Collection:

Collection is the process of gathering information from various sources for analysis and decision-making. It involves methods like surveys, interviews, sensors, or software to collect data in forms such as numbers, text, or images.

Usage:

Data has many uses like offering services, making products better, customizing content, and doing analytics.

- To understand customer preferences and improve products or services.
- To track student performance and enhance learning methods.
- To monitor patient health and develop treatments.
- To train AI models or enhance apps and systems.

6.2 Risks of Sharing Private Information

Sharing private information can make identity theft more likely. Identity theft happens when someone uses your personal details, like your name or credit card info, without permission for fraud. It can lead to big problems like losing money and harming your reputation. Thieves usually get personal info through various ways.

Phishing:

Scammers may send fraudulent emails, texts, or messages that appear to be from trusted organizations. Scammers asking you to provide personal information like passwords or financial details.

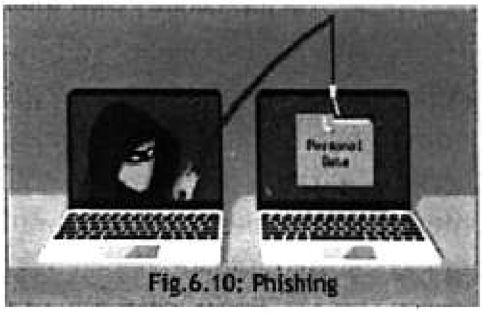


Fig.6.10: Phishing

Fig.6.11: Data Breaches

Data breaches:

When organizations or websites are attacked online, they might lose customer data, and if you're one of their customers, your data could be at risk too. Identity thieves might try to trick people into giving away personal information by pretending to be someone trustworthy.

Lost or stolen items:

Physical items like wallets, laptops, or documents containing personal information can be lost or stolen and then used by identity thieves.

Fig.6.12: Lost or Stolen Items

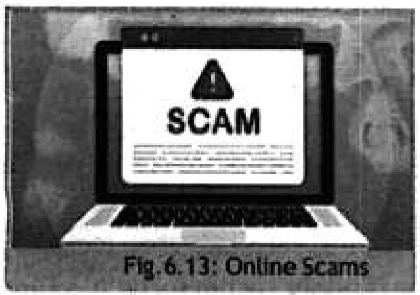


Fig.6.13: Online Scams

Online scams:

Scammers make fake websites or ads online to fool people into giving personal information or paying money to the wrong places.

6.3 Best Practices to Prevent Identity Theft

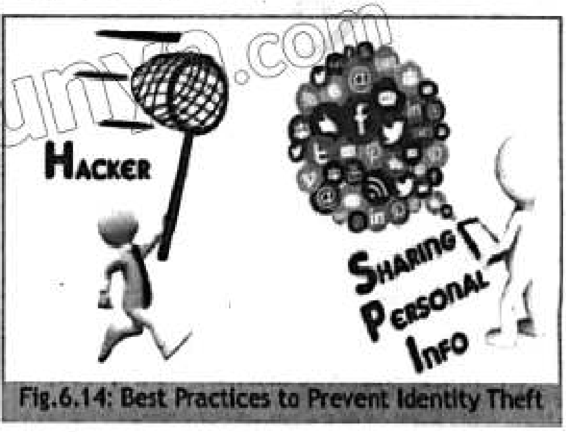


Fig.6.14: Best Practices to Prevent Identity Theft

Be careful about sharing personal information, especially if asked through email, phone, or social media. Use strong, unique passwords for your online accounts and consider a password manager to keep track of them. Enable multi-factor authentication (MFA) for extra security. Regularly check your financial statements and credit reports for unusual activity. Protect physical items with sensitive information, like IDs, passports, and credit cards. Learn about common scams and be cautious with unfamiliar people or organizations. Staying alert helps reduce the risk of identity theft and protects your personal information.

6.4 Cyber-attacks

Cyberattacks put both people and organizations at risk by targeting their security and privacy. They come in different forms like DDoS attacks which overwhelm systems with traffic; ransomware, which encrypts files and demands a ransom; and spyware, which secretly gathers information. Viruses, phishing, and various types of malwares also pose significant threats.

Staying informed and implementing strong cybersecurity measures can help protect against these risks.

Fig.6.15: Cyber-attacks

6.4.1 Types of cyber-attacks:

Certainly, there are various types of cyberattacks that threaten the security and privacy of individuals and organizations.

DDoS (Distributed Denial of Service) Attack:

A DDoS (Distributed Denial of Service) attack is when many infected computers work together to flood a website or system with too much traffic. This overloads the target, making it slow or completely unavailable to regular users.

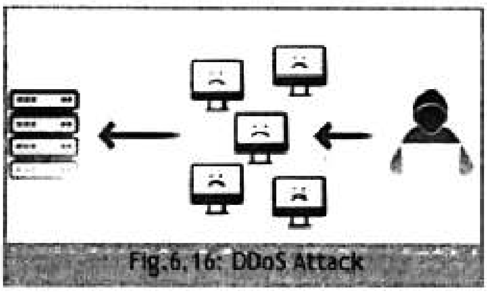


Fig.6.16: DDoS Attack

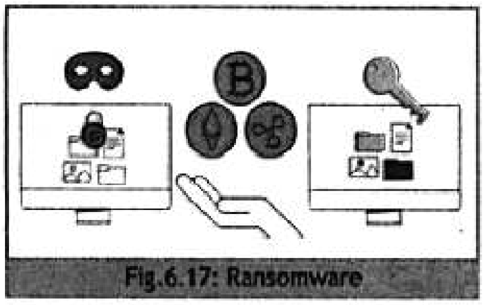


Fig.6.17: Ransomware

Ransomware:

Ransomware is a type of malicious software that locks or encrypts your files so you cannot access them. The attackers then demand money (a ransom) to unlock or decrypt your files.

Spyware:

Spyware is harmful software that secretly collects information about someone without them knowing. It can track what you type, take screenshots, or watch your online activities, and then send this data to a remote attacker.

Fig.6.18: Spyware

Viruses:

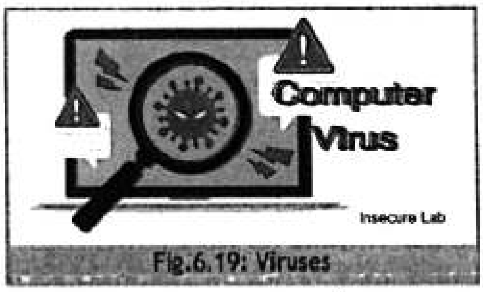


Fig.6.19: Viruses

Viruses are programs that copy themselves and infect a computer's files or software. They can spread to other systems when infected files are shared. Viruses can cause various problems, such as corrupting data or crashing the system.

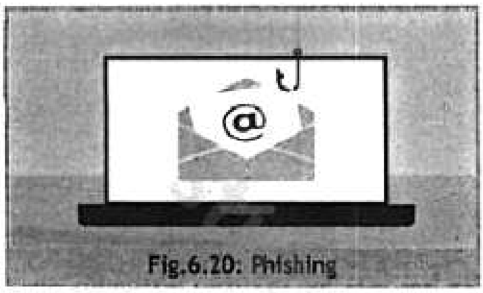


Fig.6.20: Phishing

Phishing:

Phishing attacks deceive people into giving away sensitive details like passwords or credit card numbers by pretending to be a reliable source. These attacks usually use fake emails, websites, or messages.

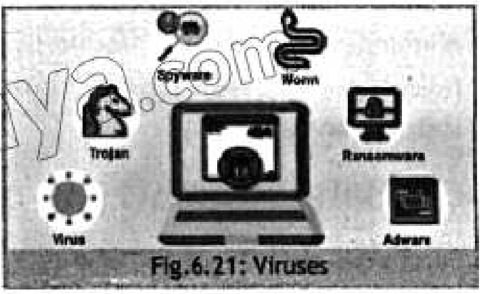


Fig.6.21: Viruses

Malware (Malicious Software):

Malware refers to harmful software like viruses, spyware, and Trojans, which can damage computer systems or steal information.

6.5 Security Methods

Fig.6.22: Cyber-attacks

Two-Factor Authentication (2FA) and Biometric Verification improve security by requiring multiple forms of ID. 2FA needs two separate factors, like a password and a phone app, to confirm identity. If one factor is breached, the other still offers protection. Biometric Verification uses unique physical features, like fingerprints or face scans, for identification. It is convenient and tough to fake but may raise privacy issues. Using both methods together provides strong protection for accessing systems and data.

6.5.1 Two-Factor Authentication (2FA):

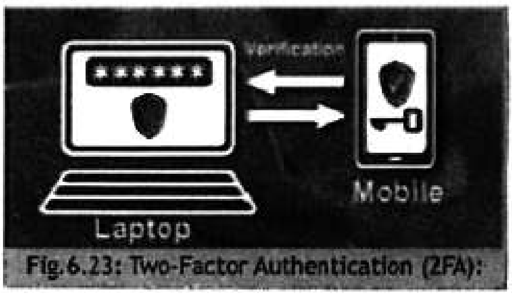


Fig.6.23: Two-Factor Authentication (2FA):

Two-factor authentication (2FA) enhances security by requiring two separate forms of identification to access a system, account, or app. It usually combines:

1. Something you know, like a password or PIN.

2. Something you have, such as a smartphone, token, or smart card.

3. Something you are, like a fingerprint or facial recognition.

This approach ensures that if one factor (e.g., a password) is compromised, an attacker would still need the second factor to gain access.

6.5.2 Biometric Verification:

Fig.6.24: Biometric Verification

Biometric verification uses a person's unique physical or behavioral traits to confirm their identity. This includes fingerprints, facial features, iris patterns, voice, and even typing or walking patterns.

To access a system or device, users provide a biometric sample, such as a fingerprint or face scan. The system then checks this sample against stored data to see if it matches. Biometric verification is convenient because it eliminates the need for passwords or PINs and is hard to fake. However, it raises privacy concerns due to the sensitive nature of biometric data and how it is stored and used.

6.6 Safe Transmission of Data

Safe data transmission involves securing information as it moves between locations. Cryptography is crucial in this process, converting readable data (plaintext) into an unreadable format (ciphertext) that only authorized users can decode. This ensures the data stays private and unchanged. Common methods include symmetric and asymmetric encryption, and protocols like SSL/TLS, which protect data in transit and prevent unauthorized access or tampering.

6.6.1 Cryptography:

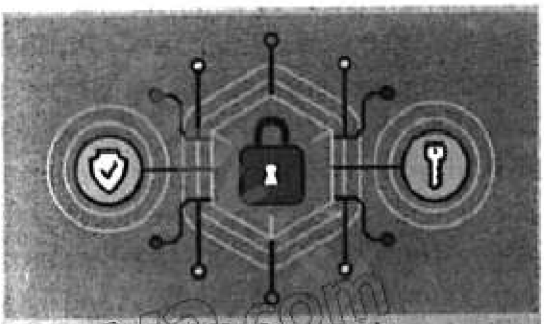


Fig.6.25: Cryptography

Cryptography is the practice of securing communication and data by transforming it into a form that only authorized parties can read. It involves key concepts like plaintext (original message), ciphertext (encrypted message), encryption (converting plaintext to ciphertext), decryption (converting ciphertext back to plaintext), and keys (secret parameters for encryption and decryption). Cryptography can be symmetric, using the same key for encryption and decryption, or asymmetric, using a pair of keys (public and private). Various ciphers, both simple and modern, ensure data integrity and security, making cryptography essential for protecting information.

6.6.2 Types of Cryptography:

Symmetric Cryptography:

Symmetric cryptography uses the same key to encrypt and decrypt data. It is fast and efficient, ideal for large data volumes. The key must be securely shared, as anyone with it can access the encrypted data.

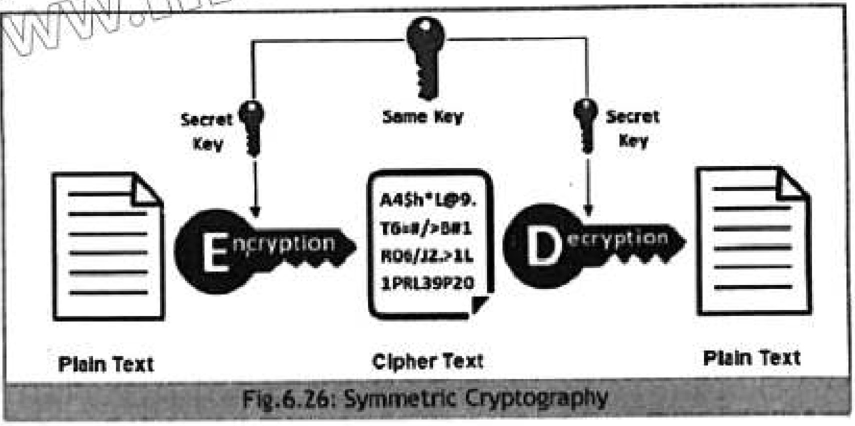


Fig.6.26: Symmetric Cryptography

Asymmetric Cryptography:

Asymmetric cryptography, or public-key cryptography, works with two keys: a public one for encryption and a private one for decryption. This setup enables secure communication without sharing a secret key. While slower than symmetric cryptography, it offers benefits like key distribution and digital signatures for authentication.

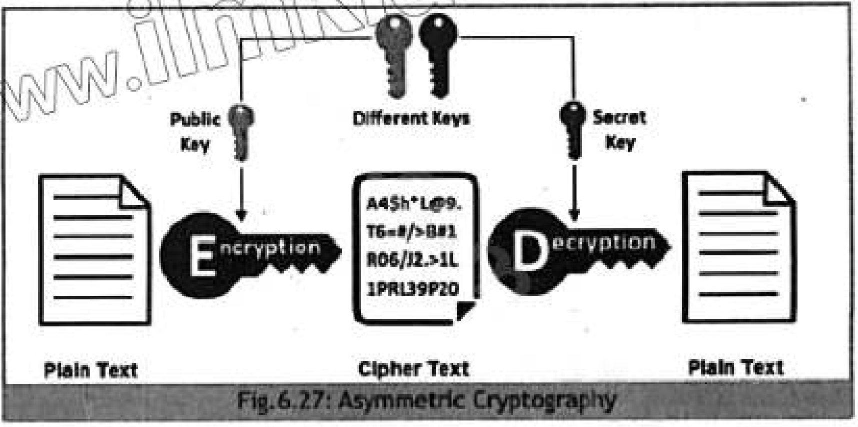


Fig.6.27: Asymmetric Cryptography

6.6.3 Popular Cipher Methods:

Caesar Cipher:

The Caesar Cipher is a simple encryption method where each letter is shifted by a fixed number of positions in the alphabet. For instance, with a shift of 3, 'A' becomes 'D', 'B' becomes 'E', and so forth. It's a basic substitution cipher and among the oldest encryption techniques.

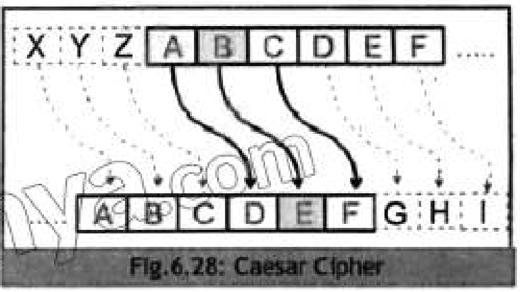


Fig.6.28: Caesar Cipher

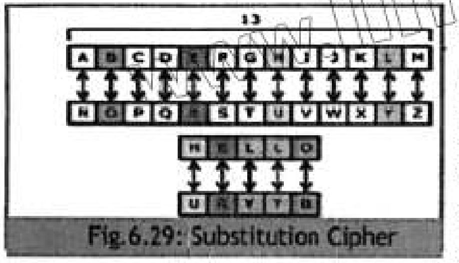


Fig.6.29: Substitution Cipher

Substitution Cipher:

A substitution cipher encrypts by replacing each letter in the plaintext with a different letter. This uses a fixed system called a substitution alphabet. The Caesar Cipher is one type of substitution cipher, but many other substitution alphabets can be used.

Transposition Cipher:

A transposition cipher encrypts by rearranging the positions of characters in the plaintext according to a specific system, without changing the characters themselves. This means the original text is reordered based on a particular pattern.

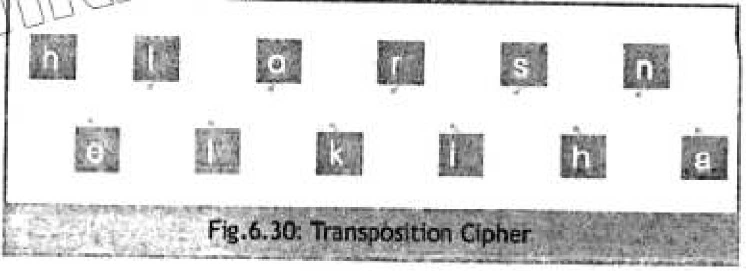


Fig.6.30: Transposition Cipher

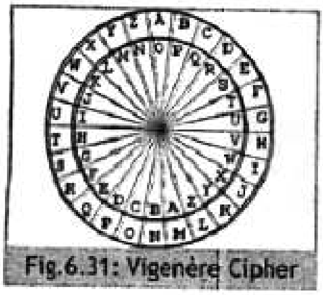


Fig.6.31: Vigenère Cipher

Vigenère Cipher:

The Vigenère cipher is a way to hide a message by changing its letters. It uses a keyword to decide how much to change each letter. Each letter in the message is changed based on a matching letter in the keyword, which is repeated as needed.

6.7 Security Protocols

Security protocols are rules and procedures to protect data and communication on networks. They keep sensitive information, like passwords, private and safe from unauthorized access. These protocols also verify user identities and ensure data remains unchanged during transmission. Examples include HTTPS for secure browsing and SSL/TLS for secure data exchange.

6.7.1 Types of protocols:

Transport Layer Security (TLS)/Secure Sockets Layer (SSL):

TLS and its predecessor SSL are cryptographic protocols used to secure internet communication. They offer encryption and authentication to ensure that data between a client and server is confidential and unaltered. TLS is commonly used in web browsers, email clients, and many online services.

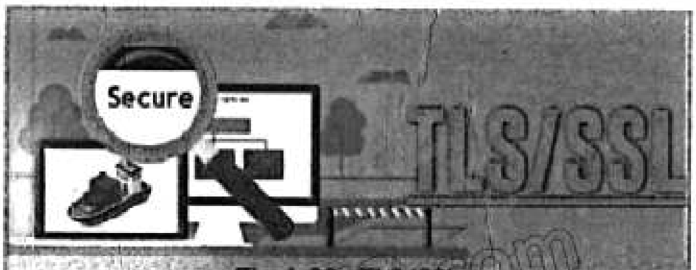


Fig.6.32: TLS/SSL

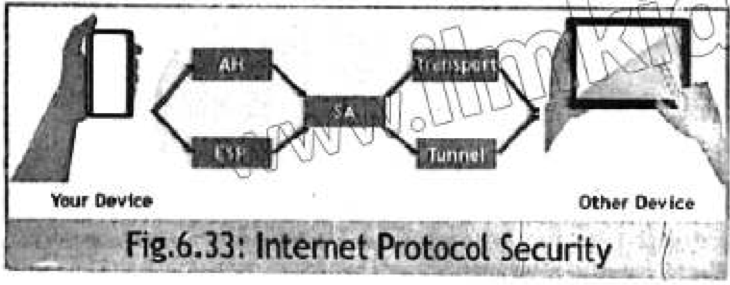


Fig.6.33: Internet Protocol Security

Internet Protocol Security (Ipsec):

IPsec is a set of protocols that secure Internet Protocol (IP) communication. It is often used for VPNs and helps establish secure communication channels between networks, remote clients, and gateways.

SSH (Secure Shell):

SSH is a protocol for secure remote access to servers and network devices. It offers strong authentication and encrypted communication, making it essential for secure system administration.

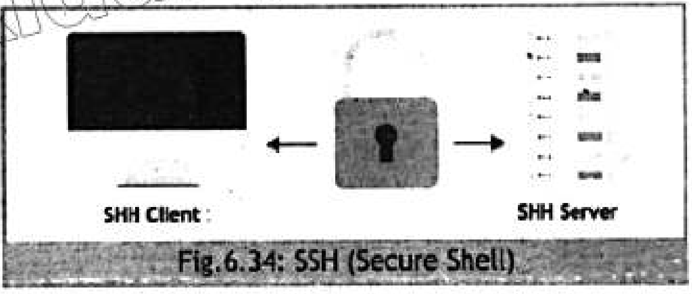


Fig.6.34: SSH (Secure Shell)

Secure File Transfer Protocols:

Secure file transfer protocols safeguard files during transmission across networks. SFTP (SSH File Transfer Protocol) encrypts data for secure and private transfers. FTPS (FTP over SSL) utilizes SSL/TLS encryption to protect files during transfer. Both methods ensure files are transmitted securely, making interception or alteration difficult.

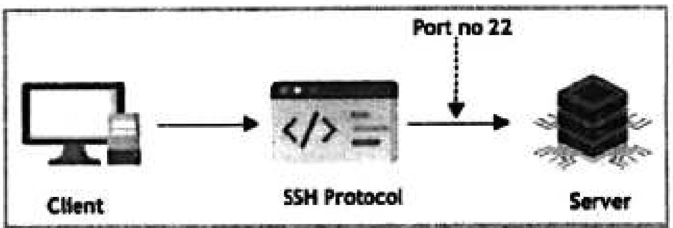


Fig.6.35: Secure File Transfer Protocols

HTTPS (Hypertext Transfer Protocol Secure):

HTTPS (Hypertext Transfer Protocol Secure) is an extension of HTTP used for secure communication over a computer network, typically the internet. It encrypts data exchanged between a web browser and a website, ensuring that sensitive information, such as passwords or payment details, remains confidential and protected from eavesdropping or tampering.

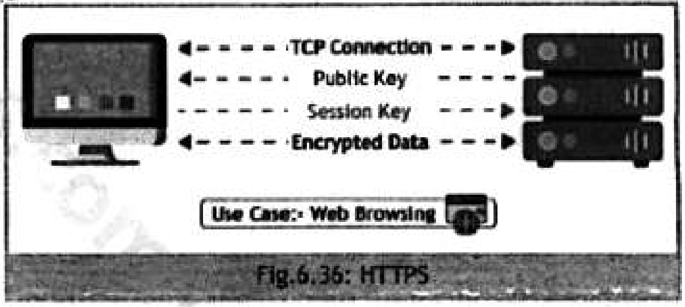


Fig.6.36: HTTPS

6.8 Troubleshoot Security Problems

Troubleshooting security problems means finding and fixing issues to protect systems and apps. It is crucial for safeguarding organizational data and assets. Steps like understanding the setup, checking logs, and running vulnerability tests help address security worries. Following best practices such as keeping software updated, educating users, and planning for incidents boosts overall security and lowers risks. Remember, security is an ongoing process needing constant assessment and adjustment to tackle changing threats. Here are some simple steps and good ways to help you find and fix security issues.

Fig.6.37: Troubleshoot Security Problems

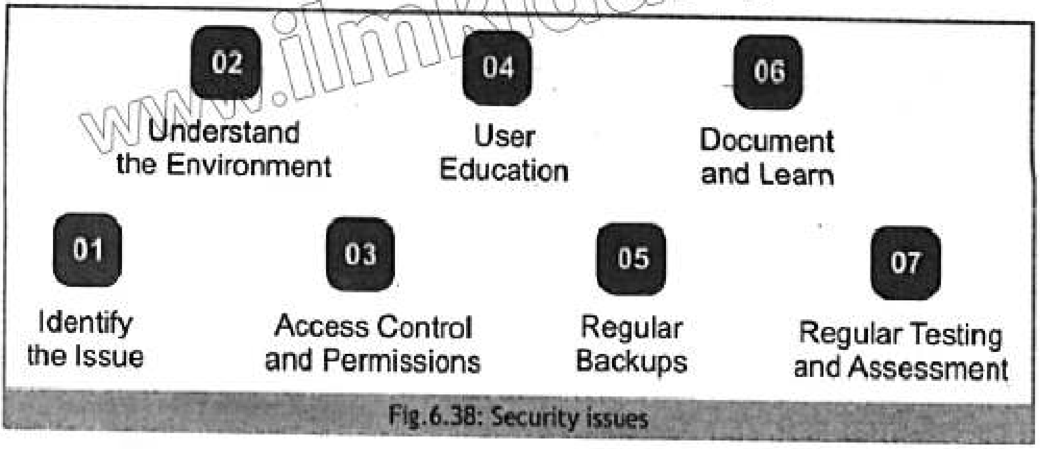

02
Understand the Environment
04
User Education
06
Document and Learn
01
Identify the Issue
03
Access Control and Permissions
05
Regular Backups
07
Regular Testing and Assessment

Fig.6.38: Security issues

- **Identify the Issue:**

  Start by clearly defining and understanding the security problem. Gather all available information about the symptoms and the systems or applications involved.

- **Understand the Environment:**

  Learn about the systems and apps, like how they're set up, what they need to work, and how they're linked in the network. This knowledge will help find weaknesses and ways attackers might try to get in.

- **Access Control and Permissions:**

  Check access control lists, user permissions, and roles to ensure that only authorized users have access to sensitive data and functionalities.

- **User Education:**

  Teach users and staff about security basics, like not clicking on strange emails or websites, making strong passwords, and reporting security issues quickly.

- **Regular Backups:**

  Regularly back up your data and check that you can restore it properly. This is crucial if you lose data because of security problems like ransomware attacks.

- **Document and Learn:**

  Write down what happened when you had a problem and what you did to fix it. This written record helps stop similar problems from happening again and makes security better."

- **Regular Testing and Assessment:**

  Continuously assess and test your security measures to identify and lighten emerging threats.

6.9 Identifying a Cybersecurity Threat

A common cybersecurity threat is a phishing attack. This involves tricking people into giving away sensitive information like passwords or personal data through fake emails, websites, or messages.

6.9.1 Various strategies of identifying cybersecurity threats:

Employee Training and Awareness for cybersecurity threats:

Regularly train employees about cybersecurity to help them spot phishing attempts. Encourage them to be cautious of unexpected emails, especially those asking for sensitive information or containing suspicious links or attachments.

Fig.6.39: Employee Training and Awareness

Fig.6.40: Email Filtering and Anti-Phishing Software

Email Filtering and Anti-Phishing Software:

Use strong email filters to catch and block phishing emails. Anti-phishing software can scan emails and spot threats before they reach employees' inboxes.

Secure Communication Protocols:

Use HTTPS for websites and encrypted email services to keep communication secure. Make sure employees check that websites and email senders are genuine before sharing sensitive information.

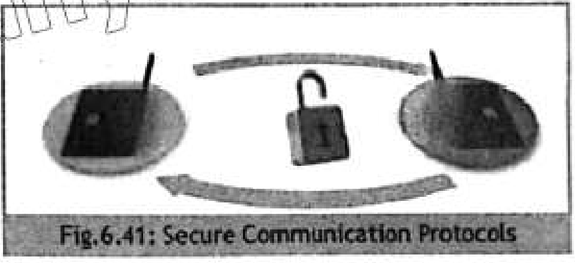


Fig.6.41: Secure Communication Protocols

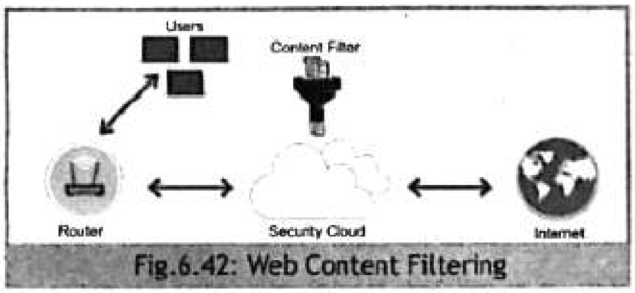


Fig.6.42: Web Content Filtering

Web Content Filtering:

Set up web filters to block access to known phishing sites and harmful content.

Security Updates and Patch Management:

Regularly update all software, operating systems, and applications with the latest security patches. Keeping everything up to date reduces the chances of attacks. These strategies help lower the risk of phishing attacks and improve overall cybersecurity. Stay informed about new threats and adjust your security measures as needed.

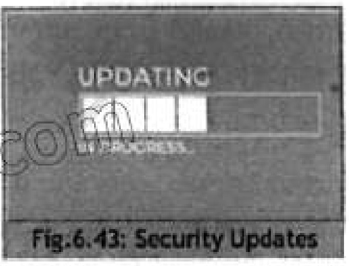


Fig.6.43: Security Updates

6.10 Computational Perspectives

Computational perspectives involve using computers to solve problems by breaking down complex tasks into simple steps. This approach helps us create efficient solutions and innovate. Learning these skills enhances problem-solving and critical thinking, preparing us for future careers.

6.10.1 The significance of Computational Perspective

Fig.6.44: Computing application

Computational perspectives are essential for students' future careers. As technology advances, computational thinking helps students solve complex problems efficiently. It promotes innovation, critical thinking, and adaptability, which are crucial in today's job market. By learning these skills, students can excel in various fields and stay competitive in a digital world.

6.11 Computing Applications

The need for collaborations to improve designs of computing applications is essential. When diverse teams work together, they combine their unique skills, experiences, and perspectives, leading to more innovative and user-friendly software. Collaboration fosters creativity and ensures that applications meet the needs of a wider audience. It also allows for resource sharing and more effective problem-solving, enhancing the overall quality of the final product.

6.11.1 The Importance of Collaboration in Enhancing Computing Application Design

Collaborations are essential for improving the designs of computing applications. By working together, diverse teams can combine their unique skills, experiences, and perspectives to create more innovative and user-friendly software. Here's why collaboration is crucial:

Diverse Perspectives:

Collaboration gathers people from diverse backgrounds, which brings a wider range of ideas and solutions. This diversity results in more creative and effective designs that appeal to a broader audience.

Enhanced Innovation:

When people from different fields collaborate, they can combine various technologies and methods, resulting in groundbreaking innovations in computing applications.

User-Centric Design:

Including end-users and stakeholders in the design process ensures the final product meets their needs and expectations. Feedback from different users helps create more user-friendly and accessible applications.

Resource Sharing:

Working together lets us share resources like what we know, the tools we have, and the money we can use. This sharing helps things move faster and makes the final product better.

Problem Solving:

Working together helps teams solve hard problems better. Different ideas and skills make problem-solving stronger.

6.12 Resources for Equal Information Accessibility

Making things that deal with fairness in accessing information means creating tools or projects to give everyone equal access to information, no matter who they are or where they live. Here are some ideas:

Digital Libraries:

Create online libraries offering free access to educational materials like textbooks and articles. These libraries should be available to anyone with internet, helping to reduce the digital gap and encourage lifelong learning.

Fig.6.45: Digital Libraries:

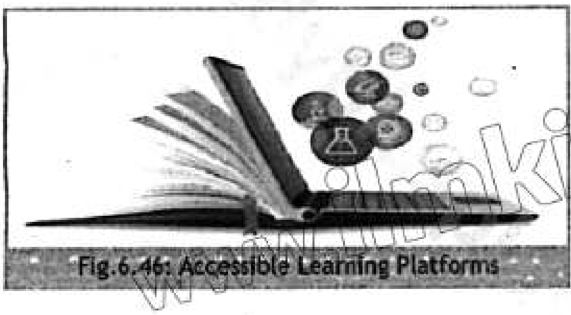


Fig.6.46: Accessible Learning Platforms

Accessible Learning Platforms:

Create e-learning platforms that cater to people with disabilities. Include tools like screen readers, captions, and alternative content formats. Ensure the platforms meet various learning needs and preferences. Make sure everyone can access educational resources equally.

Community Information Centers:

Set up community information centers with computers, internet, and learning materials. Focus on underserved communities. These centers provide access to information, skill development, and social connections. Empower individuals to engage in the digital era fully.

Fig.6.47: Community Information Centers

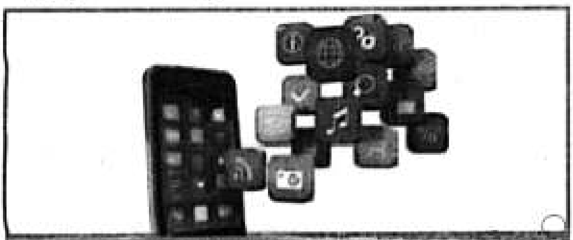


Fig.6.48: Mobile Applications

Mobile Applications:

Create phone apps for important services like healthcare or job help. These apps should be easy to use, respectful of different cultures, and in many languages to help everyone.

Open Educational Resources (OER):

Make and share open educational resources for free. These resources can be used, changed, and shared by anyone. By doing this, we make sure more people can get knowledge and help teachers and learners adapt content to what they need.

Fig.6.49: Open Educational Resources (OER)

Digital Literacy Programs:

Start programs that teach people how to use the internet wisely. They'll learn to find reliable info, use digital tools safely, and protect their privacy. These programs help people think carefully and get involved online.

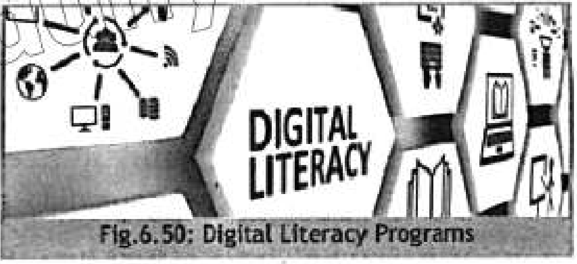


Fig.6.50: Digital Literacy Programs

Fig.6.51: Partnerships and Collaborations

Partnerships and Collaborations:

Encourage teamwork between government, schools, non-profits, and businesses to fix problems in information access and make it fair for everyone. By working together, they can make big plans to help people who do not have enough access. These ideas can help everyone get the information they need for school, work, or anything else, no matter how much money they have or other problems they face.

6.13 Collaborative Tools

Collaborative tools are software applications designed to facilitate teamwork and communication among individuals who may be working remotely or across different locations. These tools provide features that allow team members to work together on projects, share information, and communicate effectively. Below is a summary of some well-known collaborative tools.

Google Drive:

Google Drive is a service for storing and sharing files online. It lets you save documents, spreadsheets, and presentations in the cloud. You can work together with others in real-time, editing files together and seeing changes as they happen.

Fig.6.52: Google Drive

Fig.6.53: Slack

Slack:

Slack is a messaging app where teams can communicate in channels based on topics or projects. You can send direct messages, share files, and connect with other tools and services.

Trello:

Trello is a tool for managing projects using boards, lists, and cards. You can make boards for different projects, add tasks as cards, and move them as they progress. It also lets teams collaborate by adding comments, attachments, and due dates.

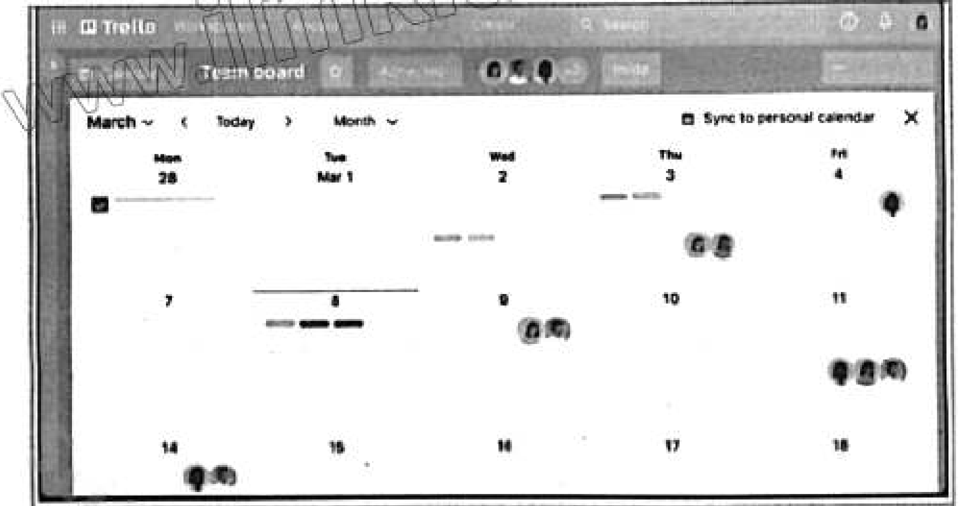


Fig.6.54: Trello

Microsoft Teams:

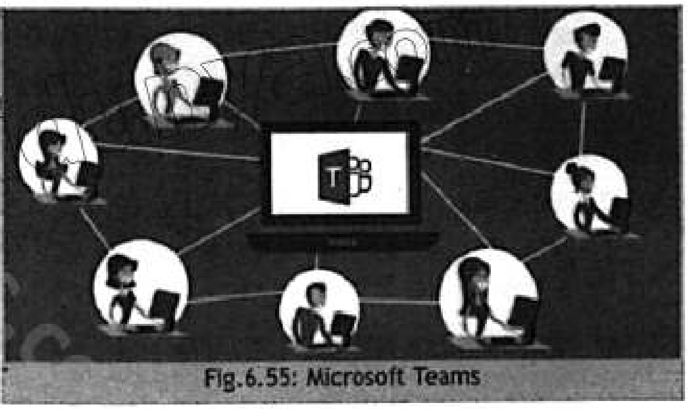


Fig.6.55: Microsoft Teams

Microsoft Teams is a collaboration platform that integrates chat, video meetings, file storage, and application integration. It allows users to communicate and collaborate in real time, share files and documents, and work together on projects.

Zoom:

Zoom is a video conferencing platform that enables virtual meetings, webinars, and conference calls. It offers features such as screen sharing, chat, and recording, making it suitable for remote collaboration and communication.

Fig.6.56: Zoom

Summary

- **Confidentiality:** Security protocols, like encryption, keep data confidential. Encryption changes data into a format only accessible by authorized parties with decryption keys. This stops unauthorized individuals from accessing sensitive information.
- **Data Integrity:** Security protocols help maintain data integrity by ensuring that data remains unchanged during storage and transmission.
- **Authentication:** Security protocols use authentication to verify user or device identities. This ensures that only authorized people or systems access or send data.
- **Access Control:** Security protocols enable access control mechanisms. These controls decide who can access, change, or send data. It ensures only authorized users access data, systems, and places.
- **Secure Transmission:** Sending data online can be risky because hackers might try to spy. However, tools like "SSL/TLS" for websites and "VPNs" for remote connections encrypt your data, making it like a secret code that only you and the intended recipient can understand.
- **Data Backup and Recovery:** Data security protocols cover backup and recovery. Regular backups and secure storage rules make sure data can be brought back if it's lost due to hardware failure or a cyberattack.
- **Phishing:** Scammers may send fraudulent emails, texts, or messages that appear to be from trusted organizations. Scammers ask you to provide personal information like passwords or financial details.
- **Data Breaches:** When organizations or websites are attacked online, they might lose customer data, and if you're one of their customers, your data could be at risk too. Identity thieves might try to trick people into giving away personal information by pretending to be someone trustworthy.
- **Online Scams:** Scammers make fake websites or ads online to fool people into giving personal information or paying money to the wrong places.
- **Cyber-attacks:** Cyberattacks put both people and organizations at risk by targeting their security and privacy.
- **DDoS (Distributed Denial of Service) Attack:** A DDoS (Distributed Denial of Service) attack is when many infected computers work together to flood a website or system with too much traffic.
- **Ransomware:** Ransomware is a type of malicious software that locks or encrypts your files so you cannot access them.
- **Spyware:** Spyware is harmful software that secretly collects information about someone without them knowing.

- **Viruses:** Viruses are programs that copy themselves and infect a computer's files or software. They can spread to other systems when infected files are shared.
- **Phishing:** Phishing attacks deceive people into giving away sensitive details like passwords or credit card numbers by pretending to be a reliable source. These attacks usually use fake emails, websites, or messages.
- **Malware (Malicious Software):** Malware refers to harmful software like viruses, spyware, and Trojans, which can damage computer systems or steal information.
- **Two-Factor Authentication (2FA):** Two-factor authentication (2FA) enhances security by requiring two separate forms of identification to access a system, account, or app.
- **Biometric Verification:** Identification method using unique physical features, like fingerprints or facial recognition, for security purposes.
- **Symmetric Cryptography:** Encryption method using the same key for both encryption and decryption of data, known for its speed and efficiency.
- **Asymmetric Cryptography:** Encryption method using a pair of keys (public and private) for encryption and decryption, offering secure communication without sharing a secret key.
- **Caesar Cipher:** An ancient encryption method where each letter in the plaintext is shifted by a fixed number of positions in the alphabet.
- **Substitution Cipher:** Encryption method replacing each letter in the plaintext with a different letter according to a fixed system.
- **Transposition Cipher:** Encryption method rearranging the positions of characters in the plaintext without changing the characters themselves.
- **Vigenère Cipher:** Encryption technique using a keyword to shift letters in the plaintext, providing a more complex substitution pattern.
- **Transport Layer Security (TLS):** Cryptographic protocol used to secure internet communication, ensuring data confidentiality and integrity.
- **Secure Sockets Layer (SSL):** Predecessor to TLS, used for securing data transmission over the internet.
- **Internet Protocol Security (IPsec):** Protocol suite for securing IP communications by authenticating and encrypting each IP packet.
- **Secure Shell (SSH):** Protocol providing secure remote access to servers and network devices, offering strong authentication and encrypted communication.
- **Hypertext Transfer Protocol Secure (HTTPS):** Extension of HTTP used for secure communication over a computer network, encrypting data exchanged between a web browser and a website.

- **Phishing Attack:** Cybersecurity threat involving tricking individuals into giving away sensitive information through fake emails, websites, or messages.
- **Digital Libraries:** Online repositories offering free access to educational materials like textbooks and articles to reduce the digital gap.
- **Accessible Learning Platforms:** E-learning platforms designed to cater to people with disabilities, including tools like screen readers and captions.
- **Community Information Centers:** Centers providing access to computers, the internet, and learning materials, especially in underserved communities.
- **Open Educational Resources (OER):** Free, accessible educational materials that can be used, modified, and shared by anyone.
- **Google Drive:** Cloud storage service allowing real-time collaboration on documents, spreadsheets, and presentations.
- **Slack:** Messaging app facilitating team communication through channels based on topics or projects.
- **Trello:** Project management tool using boards, lists, and cards to organize tasks and facilitate team collaboration.
- **Microsoft Teams:** Collaboration platform integrating chat, video meetings, file storage, and application integration for real-time teamwork.
- **Zoom:** Video conferencing platform enabling virtual meetings, webinars, and conference calls, with features like screen sharing and recording.

Exercise

Select the best answer for the following Multiple-Choice Questions (MCQs).

1. What is the primary purpose of security protocols?

    a. To speed up data transmission

    b. To protect data and prevent unauthorized access

    c. To lower the cost of data transmission

    d. To improve the appearance of web pages

2. What technique is used by security protocols to maintain confidentiality?

    a. Authentication b. Encryption c. Data backup d. Data recovery

3. Which method ensures data integrity during transmission?

    a. Encryption b. Hashing and digital signatures

    c. Phishing d. File sharing

4. Which of the following verifies user or device identity?

    a. Access control b. Encryption c. Authentication d. Data recovery

5. What do security protocols use to control who can access or modify data?

    a. Authentication b. Access control c. Malware protection d. Cryptography

6. What type of software protects against malware and viruses?

    a. Digital signatures b. Firewalls and anti-malware tools

    c. Access control mechanisms d. SSL/TLS

7. Which of the following is an example of a type of cyberattack mentioned in the text?

    a. Authentication b. Ransomware c. Access Control d. Hardware failure

8. What does Two-Factor Authentication (2FA) typically combine?

    a. A password and encryption b. A password and a secondary form of ID

    c. An IP address and encryption d. A virus scan and a firewall

9. What is an example of asymmetric cryptography?

    a. Sharing a common key for encryption

    b. Using public and private keys

    c. Using the same key for encryption and decryption

    d. Changing data transmission speed

10. Which security protocol is commonly used to secure internet communication?

    a. TLS/SSL b. FTP c. UDP d. HTTP

11. Which cipher shifts each letter by a fixed number in the alphabet?

    a. Vigenère cipher b. Transposition cipher c. Caesar cipher d. Substitution cipher

12. Which security protocol is used for secure remote access?

    a. Ipsec b. SSH c. HTTP d. FTP

13. What is phishing?

    a. A type of encryption method

    b. An attack where fake emails trick users into giving sensitive information

    c. A method to secure data transmission

    d. A secure file transfer protocol

14. Which best practice can help prevent identity theft?

    a. Sharing passwords with trusted individuals b. Using strong, unique passwords

    c. Storing all sensitive information in the cloud d. Ignoring financial statements

15. What does cryptography protect?

    a. Physical hardware b. Data and communication

    c. Marketing strategies d. System updates

16. Which of the following is an example of a security method used to enhance user authentication?

    a. DDoS attack b. Spyware

    c. Biometric verification d. Phishing

17. Which of the following tools is commonly used to support online collaboration in computing projects?

    a. Photoshop b. Google Drive

    c. Excel d. VLC Media Player

Give short answers to the following Short Response Questions (SRQs).

1. Why is it important to apply security measures when using online platforms?
2. What are the main functions of security protocols in today's digital world?
3. What are the key reasons for using security protocols to protect data?
4. How can sharing private information lead to identity theft?
5. What are the benefits and potential privacy issues of biometric verification?
6. What does Two-Factor Authentication (2FA) require for user identification?
7. Name one advantage and one disadvantage of Biometric Verification.
8. What is the primary purpose of cryptography in data transmission?
9. Describe the Caesar Cipher in brief.
10. What protocol is used for secure communication over the internet?
11. Why is it important to understand how and when your information is collected and used online?

12. Why is collaboration important in the design of computing technologies, especially when addressing equity in access to information?

Give long answers to the following Extended Response Questions (ERQs).

1. How do security protocols ensure data protection in today's digital world, and what specific techniques and measures do they employ to maintain confidentiality, and authentication?
2. What are the primary risks associated with sharing private information online, and how can individuals protect themselves against identity theft?
3. How do different types of cyber-attacks, such as DDoS, ransomware, spyware, viruses, and phishing, threaten the security and privacy of individuals and organizations?
4. Discuss the process and benefits of Biometric Verification, as well as the privacy concerns associated with it.
5. Describe how cryptography ensures the safe transmission of data, detailing the difference between symmetric and asymmetric encryption.
6. Compare and contrast the different types of cryptographic methods mentioned, including their use cases and efficiency.
7. Imagine you are developing a new mobile application that stores user data. Explain how you would ensure the security of the data during both storage and transmission.
8. You are working with a diverse team to develop a new educational website. Describe how you would use online collaborative tools and communication strategies to ensure all team members can contribute equally.

Activity 1: Identify and Apply Safe Practices

Objective: Help participants understand and implement safe practices for collaborating on digital platforms.

Materials Needed:

- Internet-connected devices
- Access to an online collaboration tool (e.g., Google Drive)

Instructions:

- Briefly explain safe practices for online collaboration, such as using strong passwords and recognizing phishing attempts.
- In small groups, have participants identify three safe practices and apply them to an online collaboration tool.
- Each group will present their implemented practices and explain their importance.

Activity 2: Discuss Security Threats and Mitigation

Objective: Educate participants on security threats and mitigation strategies.

Materials Needed:

- Handouts or digital guides on 2FA, biometric verification, and secure data transmission

Instructions:

- Briefly discuss common security threats, including phishing, malware, and data breaches.
- Divide participants into groups and assign each group one threat to focus on.
- Groups will research mitigation strategies such as 2FA, biometric verification, or secure data transmission, and present their findings to the class.

Activity 3:Collaborate on Strategies for Equity and Access

Objective: Develop strategies to ensure equitable access to information on digital platforms.

Materials Needed:

- Whiteboard or online collaborative tool (e.g., Jamboard)

Instructions:

- Discuss the importance of equity and equal access to information.
- In small groups, brainstorm strategies to provide equitable access, such as ensuring all participants have the necessary technology and skills.
- Each group presents their strategies, and the class discusses how to implement them in various digital collaboration scenarios.