



CHAPTER-9

CYBERSECURITY AND SAFE DIGITAL COLLABORATION

Introduction:

In this chapter, students will explore how technology supports safe, secure, and responsible participation in the digital world. They will learn about online safety, cybersecurity, data protection, privacy settings, and secure collaboration using modern digital platforms.

9.1 Safe and Responsible Digital Practices

Ex. 0.1: What is online safety? Explain the importance of online safety and describe how strong passwords and safe browsing habits protect personal data.

Online Safety

Online safety means protecting yourself and your information while using the internet. Online safety includes being careful about what you share, where you click, and how you store your data. Every action performed on the internet leaves a digital footprint that can be tracked.

Importance of Online Safety

- It prevents identity theft and fraud.
- It protects personal and school-related information from misuse.
- It reduces risk of scams, viruses, and cyber threats.
- It keeps your online reputation and privacy intact.

Short Question

What is Online safety and why is it important?

Strong Passwords and Their Role in Data Protection

A strong password is a combination of letters, numbers, and symbols that helps protect your accounts from hackers.

- i. A strong password contains a mix of letters, numbers, and symbols. This makes it difficult for hackers to guess the password.
- ii. A different password for each account reduces the chance of all accounts being hacked if one password is stolen.
- iii. Do not use personal information such as your name or birthday as a password because it is easy to guess.
- iv. Passwords should be changed regularly to improve account security.
- v. Never share your password with other people because it protects your personal information.
- vi. A strong password is the first line of defense for protecting important files and online data.

Example: A password like Ahsan@2026! is stronger than ahsan123 because it contains letters, numbers, and symbols.

Safe Browsing Habits and Their Role in Data Protection

Safe browsing habits help protect personal data by avoiding harmful websites, downloads, and online scams.

- i. Programs and files should be downloaded only from trusted websites.
- ii. Do not click unknown links or pop-up advertisements because they may lead to fake websites or malware.
- iii. Always check the website address before entering personal information.
- iv. Always verify the website and source before downloading any file.
- v. Using antivirus software provides extra protection against harmful files and unsafe websites.
- vi. Safe browsing habits reduce the risk of viruses, scams, identity theft, and unauthorized access to personal information.



DO YOU KNOW?

- A strong password with 12 characters can take millions of years for a computer to crack, but a weak one can be cracked in seconds.



TIDBIT

- Understanding threats and preventive measures, reduces the chance of cybercrime.

Ex.O.2: Discuss the role of software updates and security patches in maintaining computer security, and explain the risks associated with outdated software.

Software Maintenance and Updates

Software maintenance means keeping programs and applications in good working condition by updating them regularly. Software updates fix errors, improve performance, and add new features.

Security patches are special software updates that fix security weaknesses in a program. They close security gaps that hackers may exploit. Installing software updates and security patches helps keep computers secure, reliable, and protected from cyber threats.

Example

Updating a web browser fixes security problems and improves its performance.

Short Question

What is Software maintenance and updates?

Role of Software Updates and Security Patches

- Software updates and security patches close security holes that hackers may use to attack a system.
- Updates improve the speed and performance of software and help it work more efficiently.
- Many updates include new features that make the software more useful and secure.
- Updated software reduces the risk of malware infections and data breaches.
- Regular updates make it harder for hackers to exploit known security weaknesses.
- Updates help software work properly with new operating systems and other applications.

Short Question

Why are Software updates important?

Risks of Outdated Software

- Outdated software contains security weaknesses that hackers can exploit.
- It increases the risk of viruses, malware, and data theft.
- Software may become slow, unstable, or crash frequently.
- Old software may not work correctly with newer operating systems or applications.
- Personal and important data may become vulnerable to unauthorized access.

Example

If a student keeps the operating system updated, the computer remains more secure and works properly with the latest applications.



CLASS ACTIVITY

Students compare features of updated vs outdated software and discuss how old versions can be attacked.

Ex.Q.3. Describe how privacy and security settings on online platforms can be managed. Explain why reading privacy policies is important for data protection.

Privacy and Security Settings

Privacy and security settings help users control how their personal information is collected, used, and shared on online platforms. These settings are available in most apps, websites, and online platforms. They help protect personal information such as location, contacts, and browsing history. Managing these settings prevents the misuse of personal data and makes online activities more private and secure.

Managing Privacy and Security Settings

- Users can choose who is allowed to see their posts, profile, and other personal information.
- Privacy settings allow users to decide who can send messages or contact them.
- Turning on two-factor authentication provides an extra layer of account security.
- Users should allow only the permissions that are necessary for an app to work properly.
- Privacy and security settings should be checked regularly because online platforms may update their privacy rules.

Example

On Instagram, users can make their account private so that only approved followers can see their posts. They can also turn off location sharing and enable two-factor authentication for better security.

Importance of Reading Privacy Policies

A privacy policy explains how a website or app collects, stores, uses, and shares your personal information. It is important to read the privacy policy before creating an account or accepting the terms.

- It helps users understand what information is collected and why it is collected.
- It explains how personal information is stored and used.
- It tells users whether their information is shared with advertisers or third-party services.
- It helps users decide whether they want to share their personal data.
- It protects personal data by helping users make informed decisions before using an online platform.

Example

When creating an account on a social media platform, the privacy policy may explain that it collects your name, email address, location, browsing activity, and app usage. It may also explain whether this information is shared with advertisers or third-party services.

Example

On WhatsApp, users can choose whether their profile photo is visible to everyone, only their contacts, or nobody. They can also turn off read receipts (blue ticks) so that others cannot see whether their messages have been read.



TIDBIT

- Regularly reviewing settings ensures protection as platforms update their features.

Q. What is safe online collaboration? Explain secure collaboration platforms and digital etiquette.

Safe Online Collaboration

Safe online collaboration means working together through digital tools in a secure and responsible way.

Online collaboration allows people to work together using digital tools from any location. It is important to use secure platforms and follow safety rules when sharing files or communicating online.

Short Question

What is Safe online collaboration?

Students should work responsibly in virtual groups and protect their personal and school data. Safe collaboration builds trust and supports productive and respectful teamwork.

Identifying Secure Collaboration Platforms

Secure collaboration platforms are online tools that provide a safe environment for communication and teamwork. Google Workspace and Microsoft Teams are examples of secure collaboration platforms. These platforms use encrypted communication and access controls to protect data. Students can safely share documents, attend online meetings, and communicate with each other. Using trusted and approved platforms reduces cyber risks and protects important information.

For example, students can use Google Workspace for school projects by sharing a project file only with selected classmates through restricted access. They can also use Google Meet for secure online classes, where only authorized participants are allowed to join. These features help students collaborate safely while protecting their schoolwork and personal information.

Practicing Digital Etiquette and Responsible Communication

Digital etiquette means communicating politely, respectfully, and responsibly in online environments.

- Students should use respectful and appropriate language while communicating online.
- Everyone's opinions should be respected during online discussions.
- Students should never share their private or personal information during online communication.
- Spam messages, unrelated content, and disrespectful behavior should be avoided during online discussions.
- Responsible communication helps create a positive, respectful, and professional digital environment.



Additional Multiple Choice Questions

1. Online safety means protecting yourself and your information while using the:
A) Internet B) Printer C) Scanner D) Keyboard
2. A strong password is a combination of:
A) Letters only B) Numbers only C) Letters, numbers, and symbols D) Symbols only
3. Which of the following is the first line of defense for protecting important files and online data?
A) Antivirus software B) Strong password C) Web browser D) Firewall
4. Downloading software or files from unknown websites can:
A) Improve performance B) Increase storage
C) Harm your computer or steal your personal information D) Speed up the internet
5. Software maintenance means keeping programs and applications in good working condition by:
A) Installing hardware B) Updating them regularly C) Changing passwords D) Deleting files
6. Which of the following is an important benefit of software updates?
A) They fix security gaps that hackers may exploit C) They stop the internet from disconnecting.
B) They remove the need for antivirus software. D) They permanently prevent all cyberattacks.
7. A privacy policy explains how a website or app:
A) Repairs computers B) Creates passwords
C) Collects, stores, uses, and shares your personal information D) Installs software
8. Which setting provides an extra layer of account security?
A) Auto Save B) Dark Mode C) Airplane Mode D) Two-factor authentication
9. Which of the following is an example of a secure collaboration platform?
A) Google Workspace B) Paint C) Notepad D) Calculator
10. Digital etiquette means communicating:
A) Quickly and secretly B) Politely, respectfully, and responsibly
C) Only through social media D) Without following any rules

Answers:

- | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|---|
| 1 | A | 2 | C | 3 | B | 4 | C | 5 | B | 6 | A | 7 | C | 8 | D | 9 | A | 10 | B |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|---|

9.2 Cybersecurity Awareness and Threat Management

Q. What is cybersecurity awareness?

Cybersecurity Awareness

Cybersecurity awareness means understanding how to protect computers, networks, and data from cyberattacks.

As people use technology more in daily life, cyber threats have become more common. Hackers use different tricks and harmful software to steal information or damage computer systems. Being aware of these threats helps users stay alert and use the internet safely.

Knowing how to detect, prevent, and respond to cyber threats helps protect personal and organizational data.

Short Question

What is Cybersecurity awareness?

Ex.Q.4.What are Cyber Threats? Explain different types of cyber threats such as viruses, phishing, ransomware, spyware, and DDoS attacks. Discuss how these threats can affect both individuals and organizations.

Cyber Threats

Cyber threats are actions or programs that target computers and networks to cause harm. Cyber threats can steal information, damage systems, or interrupt online services. Understanding these threats helps users recognize warning signs at an early stage.

Most cyberattacks can be avoided by safe browsing, using antivirus software, and being careful with emails and unknown links. Recognizing cyber threats is the first step in protecting digital systems.

Short Question

What are cyber threats?

Common Types of Cyberattacks

i. Virus

A virus is a harmful program that spreads through infected files and can damage or delete data.

Example: A virus can spread when a user opens an infected file downloaded from an unknown website.

ii. Phishing

Phishing is a cyberattack that tricks people into sharing passwords or personal information through fake emails or websites.

Example: A fake bank email asks a user to enter their account password on a fake website.

iii. Ransomware

Ransomware is a type of malware that locks data and demands payment to unlock it.

Example: A ransomware attack may lock all files on a computer and ask for money to restore access.

iv. Spyware

Spyware is a harmful program that secretly collects user information without permission.

Example: Spyware may secretly record usernames, passwords, or browsing activities.

v. Distributed Denial of Service (DDoS) Attack

A Distributed Denial of Service (DDoS) attack overloads a website with a large number of requests, causing it to slow down or stop working.

How Cyberattacks Affect Individuals and Organizations

Cyberattacks can cause serious harm to both individuals and organizations.

i. Loss of Personal Data

Individuals may lose important files, passwords, or personal information.

ii. Financial Loss

Cyberattacks can cause financial losses by stealing money or demanding ransom.

iii. Data Breaches

Organizations may lose sensitive data, including customer information.

Short Question

How do Cyberattacks Affect Individuals and Organizations?

iv. Loss of Customer Trust

Customers may lose trust in an organization after a cyberattack.

v. Disruption of Business Operations

Cyberattacks can stop the normal working of businesses, schools, and hospitals.

vi. Damage to Reputation

Organizations may suffer damage to their reputation because of security incidents.

TIDBIT

- Avoid offensive language, spam, and sharing confidential information.

DO YOU KNOW?

- Phishing is among the most common attacks.

Ex.Q.5: Discuss security tools and techniques like Two-Factor Authentication (2FA), biometric verification, firewalls, intrusion detection systems (IDS), and antivirus software. Explain how each helps in protecting data.

Security Tools and Techniques

Security tools and techniques are used to protect computers and networks from online threats. These tools make it difficult for hackers and malicious software to access important information. They include authentication systems, firewalls, Intrusion Detection Systems (IDS), and antivirus programs. These tools detect and block harmful activities. Using them properly keeps personal data safe and reduces the risk of cyberattacks.

1. Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) is a security method that requires two forms of verification before allowing access to an account.

For example, after entering a password, the user must provide another form of verification, such as a code sent to a mobile phone or email. This extra security step makes it much harder for hackers to access the account.

Short Question

What is Two-Factor Authentication (2FA)?

2. Biometric Verification

Biometric verification is a security method that uses physical features to verify a user's identity. It uses fingerprints, face scans, or voice patterns to confirm the identity of a user. Biometric verification provides strong protection for accounts and personal data.

3. Firewall

A firewall acts as a barrier between a computer and the internet. It allows safe data to pass through and blocks harmful network traffic. This helps protect the computer from unauthorized access.

4. Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) monitors a network for suspicious activities. It detects possible security threats and alerts users about unusual network activity.

5. Antivirus Software

Antivirus software scans files and removes viruses or malware before they can damage the system. Regular scanning helps keep computers and data safe from harmful software.

CLASS ACTIVITY

Students simulate logging into an account with a second step (code from teacher) to understand how 2FA works.

Sol:

- Student enters a username and password.
- The teacher provides a one-time verification code.
- The student enters the verification code.
- If the code is correct, the account login is successful.
- Students learn that Two-Factor Authentication (2FA) uses two verification steps to improve account

Q. What is data protection and cryptography? Explain secure methods for transmitting and storing data.

Data Protection

Data protection means keeping digital information safe from unauthorized access, loss, or damage. It ensures that only authorized people can access or use the data.

Cryptography

Cryptography is the science of securing information so that only authorized users can understand it.

It protects information from unauthorized access. Cryptography is widely used in secure websites, online banking, and messaging applications.

Example

When a message is sent over the internet, encryption converts it into coded text. If someone intercepts the message, they cannot read it without the correct key.

Short Question

What is Cryptography in data protection?

Cryptography uses two main concepts:

i. Encryption

Encryption is the process of converting readable data into coded text using a specific key. It protects information from unauthorized users during storage and transmission.

Example

When a user enters a password on a secure website, the password is encrypted before being sent over the internet.

ii. Decryption

Decryption is the process of converting coded text back into its original readable form. Only authorized users with the correct key can decrypt and read the information.

Example

When a secure message reaches the receiver, it is decrypted so the original message can be read.

Short Question

What are Encryption and decryption?

Secure Methods for Transmitting and Storing Data

Secure methods help protect data while it is stored or transferred over the internet.

i. Encrypted Connections

Encrypted connections, such as HTTPS, protect data while it is being transmitted over the internet.

ii. Encrypted Cloud Storage

Cloud storage services use encryption to protect saved files from unauthorized access.

iii. Regular Backups

Regular backups help protect data from loss caused by system failure or cyberattacks.



TIDBIT

Secure storage and transmission prevent unauthorized access and breaches.

Q. What are Intrusions? Explain detecting and preventing intrusions. How can vulnerabilities be identified and prevented?

Intrusions

Intrusions are unauthorized attempts to access, damage, or misuse a computer system, network, or data. An intrusion happens when an attacker enters a system without permission or performs harmful activities. Intrusions can steal information, install malware, change data, or disrupt services.

Short Question

What are Intrusions?

Detecting and Preventing Intrusions

Detecting and preventing intrusions means identifying and stopping unauthorized access to a computer or network. Cyber intrusions happen when hackers exploit weaknesses to steal data or damage systems. Monitoring tools and security software help detect unusual activities that may indicate an attack. Early detection helps prevent major losses and keeps systems running safely. Staying alert and regularly updating security measures helps protect computers and networks from intrusions.

Example

If antivirus software detects an unauthorized program trying to access a computer, it alerts the user and blocks the threat.

Identifying Vulnerabilities and Suspicious Activities

A vulnerability is a weakness in software, hardware, or user behavior that hackers can exploit.

Vulnerabilities

Weak software, outdated systems, or careless user actions can create security vulnerabilities.

Suspicious Activities

Suspicious activities include unexpected system slowdowns, unknown programs running, or unusual network traffic.

Checking System Logs

Regularly checking system logs helps identify unusual activities and possible security threats.

Using Scanning Tools

Security scanning tools help detect vulnerabilities and other warning signs in a computer system.

Early Detection

Finding and fixing vulnerabilities early reduces the risk of successful cyberattacks.

Applying Troubleshooting and Preventive Measures

Troubleshooting is the process of finding the cause of a security problem and fixing it.

Install Security Software

Install firewalls, antivirus software, and anti-malware software to protect the system from cyber threats.

Update Software

Regularly update software to fix security weaknesses and improve protection.

Change Passwords

Change passwords regularly, especially after a security incident, to prevent unauthorized access.

Remove Harmful Files

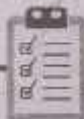
Delete infected or suspicious files to stop them from damaging the system.

Restore Data from Backups

If important data is lost or damaged, it can be restored from backups.

Document Security Problems

Keep a record of the problem and the steps taken to solve it. This helps prevent similar problems in the future.



CLASS ACTIVITY

Students look at sample system logs or screenshots to find suspicious actions.

Sol: Students examine the given system logs or screenshots carefully. They identify suspicious actions such as repeated failed login attempts, login from an unknown user, or access at an unusual time. After identifying these activities, students discuss why they may be security threats and share their observations with the class.



Additional Multiple Choice Questions

- Cybersecurity awareness means understanding how to protect:**
A) Computers, networks, and data from cyberattacks B) Mobile phones only
C) Websites only D) Software only
- Phishing is a cyberattack that tricks people into sharing:**
A) Photos and videos B) Passwords or personal information
C) Computer programs D) Internet settings
- Ransomware is a type of malware that:**
A) Speeds up computers B) Monitors network traffic
C) Locks data and demands payment to unlock it D) Improves system performance
- Two-Factor Authentication (2FA) is a security method that requires:**
A) One password only B) Two forms of verification
C) Two email accounts D) Two antivirus programs
- A firewall acts as a barrier between a computer and the:**
A) Printer B) Keyboard C) Internet D) Scanner
- Cryptography is the science of securing information so that only _____ users can understand it.**
A) Registered B) Online C) Skilled D) Authorized
- Encryption is the process of converting readable data into:**
A) Printed text B) Coded text C) Digital images D) Backup files
- Which secure method protects data while it is being transmitted over the Internet?**
A) Regular backups B) Encrypted cloud storage C) Encrypted connections (HTTPS) D) System logs
- A vulnerability is a weakness in software, hardware, or user behavior that hackers can:**
A) Upgrade B) Repair C) Monitor D) Exploit
- Which of the following is a preventive measure against cyber threats?**
A) Delete infected or suspicious files C) Ignore software updates.
B) Share passwords with friends. D) Download files from unknown websites.

Answers:

- | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|---|
| 1 | A | 2 | B | 3 | C | 4 | B | 5 | C | 6 | D | 7 | B | 8 | C | 9 | D | 10 | A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|---|

9.3 Digital Collaboration and Equity in Computing

Q. What is digital collaboration? Explain the importance of teamwork and communication in digital environments.

Digital Collaboration

Digital collaboration means using technology to work together on shared tasks, projects, or ideas. It allows people to connect and contribute from different locations using the Internet. Digital collaboration helps students and teams to complete work efficiently through teamwork, communication, and responsibility.

Short Question
What is Digital collaboration?

Equity in Computing

Equity in computing ensures that everyone, regardless of background or ability, can access and use digital resources equally. Combining digital collaboration with fairness helps create inclusive and effective learning and working environments.

Working Together Online

Working together online allows teams to share ideas, exchange feedback, and complete tasks without being in the same place. It promotes cooperation and creativity through shared documents, online discussions, and digital resources. Clear communication and mutual respect are important for successful online teamwork. Digital collaboration prepares students for modern workplaces where remote work is common. Online teamwork improves problem-solving skills and builds interpersonal skills.

Example

Students from different locations can work together on a project using shared online documents and discuss ideas through video calls.

Importance of Teamwork and Communication in Digital Environments

- Teamwork in digital environments requires clear communication and trust among team members.
- When all members share ideas and listen to others, projects can be completed smoothly.
- Effective communication reduces misunderstandings and keeps everyone informed about project progress.
- Tools like group chats, emails, and video calls help teams stay connected.
- Good teamwork encourages creativity, cooperation, and shared responsibility for achieving goals.

Tools and Platforms for Real-Time Collaboration

Real-time collaboration tools allow multiple users to work on the same project at the same time. Platforms such as Google Workspace, Microsoft Teams, and Zoom help users share documents, communicate, and conduct online meetings. These tools help teams organize tasks, edit files together, and stay updated instantly. Real-time collaboration saves time and reduces errors by keeping all team members connected and informed.



TIDBIT

- Teams that communicate clearly finish tasks faster and make fewer mistakes.

Q. Explain designing for equity and accessibility. How can inclusive applications be created for diverse users?

Designing for Equity and Accessibility

Designing for equity and accessibility means creating technology that can be used by everyone, including people with different abilities and backgrounds. Equal access means that every person should have the same opportunity to use technology and the internet. It includes access to reliable devices, internet connections, and digital skills.

Short Question

What is Designing for equity and accessibility?

Some people may face problems due to disabilities, language barriers, or limited resources. Understanding these challenges helps developers and organizations create solutions that are useful for everyone. Accessible design helps people with disabilities and also improves the overall usability of technology.

Example

A website with clear text, simple navigation, and screen reader support can be used easily by different types of users.

Creating Inclusive Applications for Diverse Users

Inclusive applications are designed to fulfill the needs of different types of users. Developers add features that make applications easier to use for people with different abilities and backgrounds. Simple designs and clear instructions help beginners understand and use applications easily.

Features of Inclusive Applications

Screen Readers

Screen readers help visually impaired users understand digital content by converting text into speech.

Subtitles for Videos

Subtitles help users understand video content, especially those who cannot hear audio clearly.

Multiple Language Options

Different language options allow more users to access and understand applications.

Simple Layouts and Clear Text

Simple layouts and clear text make applications easier to use for beginners and all types of users.

Testing with Different Users

Developers should test applications with different users to ensure that they are accessible for everyone.



CLASS ACTIVITY

Groups complete a small task, such as planning a poster, while practicing clear online-style messaging.

Sol: Students work in groups to plan a poster by communicating through clear and polite online-style messages. They use simple, respectful, and easy-to-understand language while sharing ideas and completing the task together.

Q. Explain the strategies for effective collaboration. How does reflection improve teamwork?

Strategies for Effective Collaboration

Effective collaboration helps teams to work smoothly and complete tasks successfully. Teamwork becomes stronger when every member understands their responsibilities and communicates clearly. Planning, organizing, and sharing ideas help group projects move forward without confusion. Collaboration teaches team members to respect different opinions and work together to achieve a common goal.

Assigning Roles

Clear roles help each team member understand their specific responsibilities. Each person performs a different task according to their role. One member may handle research, another may organize information, while another may prepare the final presentation.

Managing Tasks

Managing tasks helps the team complete work on time and avoid delays. Creating checklists and timelines helps members track their progress and complete assigned tasks properly.

Setting Team Goals

Setting shared goals gives team members a clear direction. When roles and goals are clear, teamwork becomes easier and more efficient. Common goals encourage cooperation and help all members work together.

Reflecting on Collaborative Experiences

Reflection means thinking about the teamwork experience after completing a project. It helps students understand what went well and what needs improvement. Team members can identify strengths, such as good communication, and weaknesses, such as missed deadlines.

Discussion to Improve Teamwork

Discussing teamwork experiences helps students learn from mistakes and become better team members. Reflection encourages respect and understanding among group members. It improves communication and helps teams achieve better results in future collaborations.



TIDBIT

➤ Clear roles, task management, and goal setting improve teamwork efficiency.



Additional Multiple Choice Questions

- Digital collaboration means using technology to work together on shared:
A) Tasks, projects, or ideas B) Computer viruses C) Hardware devices D) Operating systems
- Equity in computing ensures that everyone, regardless of background or ability, can:
A) Buy computers B) Access and use digital resources equally
C) Create software D) Repair networks
- Working together online allows teams to:
A) Share ideas, exchange feedback, and complete tasks B) Work without communication
C) Avoid teamwork D) Use only one computer

4. Which tool is used for real-time collaboration?
A) Paint B) Zoom C) Calculator D) Notepad
5. Designing for equity and accessibility means creating technology that can be used by:
A) Programmers only
B) Students only
C) Everyone, including people with different abilities and backgrounds
D) Businesses only
6. Screen readers help _____ users understand digital content by converting text into speech.
A) Hearing impaired B) Visually impaired C) Young D) Expert
7. Which feature helps users understand video content, especially those who cannot hear audio clearly?
A) Screen readers B) Multiple language options C) Subtitles for videos D) Simple layouts
8. Which strategy helps each team member understand their specific responsibilities?
A) Managing tasks B) Setting team goals C) Reflection D) Assigning roles
9. Reflection means thinking about the teamwork experience:
A) Before starting a project B) During a meeting only
C) After completing a project D) Before assigning roles
10. Why is reflection important in teamwork?
A) It reduces internet speed. C) It avoids group discussions.
B) It helps students identify strengths and weaknesses. D) It removes the need for teamwork.

Answers:

1 A 2 B 3 A 4 B 5 C 6 B 7 C 8 D 9 C 10 B

9.4 Digital Entrepreneurship and Innovation

DO YOU KNOW?

- Most successful entrepreneurs are not born risk-takers—they develop risk-taking skills through experience.

Ex.Q.6. Explain the concept of entrepreneurship and describe how digital technologies have created new opportunities for entrepreneurs. Include at least three examples of digital entrepreneurship.

Entrepreneurship

Entrepreneurship is the process of creating, managing, and growing business ideas. Entrepreneurs identify problems and provide useful products or services as solutions. They use creativity, innovation, and technology to meet customer needs. Entrepreneurship creates business opportunities and supports economic growth.

Digital Entrepreneurship

Digital entrepreneurship is the use of technology and online platforms to create, manage, and grow business ideas.

It helps individuals solve real-world problems by creating innovative digital solutions. Entrepreneurs use social media, e-commerce websites, and freelancing platforms to reach customers around the world.

Innovation helps in developing new products and services according to changing market needs. Digital entrepreneurship provides opportunities for students to convert creative ideas into successful digital businesses.

How Digital Technologies Create New Opportunities

Digital technologies create many new business opportunities.

- They help entrepreneurs reach customers around the world.
- They make it easy to promote products and services online.
- They help develop innovative products and services.
- They create new job opportunities through digital platforms.
- They allow businesses to grow with lower costs and better communication.

Short Question

What is Digital entrepreneurship?

Examples of Digital Entrepreneurship

- An online store that sells handmade products through an e-commerce website.
- A freelancer providing programming, graphic design, or digital marketing services online.
- An online learning platform that provides educational resources to students.
- A mobile app that helps farmers improve farming decisions.
- A digital payment service that makes business transactions easier and safer.

Q. Who is an entrepreneur? Describe characteristics of successful entrepreneurs.

Entrepreneur

An entrepreneur is a person who starts and manages a business to earn a profit by offering a product or service. Entrepreneurs identify opportunities, take risks, and make business decisions.

Characteristics of Successful Entrepreneurs

Successful entrepreneurs have different qualities that help them build and manage successful businesses.

Creativity

Successful entrepreneurs are creative and always search for new ideas to solve problems.

Hard Work and Commitment

Entrepreneurs work hard and remain committed to achieving their goals.

Confidence

Good entrepreneurs are confident about their ideas and decisions.

Risk Taking

Successful entrepreneurs take calculated risks after careful thinking and planning.

Decision-Making Skills

Entrepreneurs have strong decision-making skills to choose the right actions for their business.

Problem-Solving Skills

They can identify problems and find effective solutions.

Adaptability

Successful entrepreneurs can adjust to changing market conditions and customer needs.

Short Question
Describe two characteristics of successful entrepreneur?

Q. Explain entrepreneurship in Pakistan and the digital economy. How can business opportunities be identified?

Entrepreneurship in Pakistan and the Digital Economy

Entrepreneurship in Pakistan is growing due to increased access to the internet and mobile technology. Many young people are starting online businesses through social media, e-commerce platforms, and freelancing websites. The digital economy is creating new job opportunities in fields such as software development, digital marketing, and online services. Government and private initiatives are also supporting startups and innovation. This growth helps improve the economy and encourages young people to become job creators instead of job seekers.

Example

A young person starts a freelancing business and provides online services to customers in different countries.

Identifying Business Opportunities

Identifying business opportunities means finding problems in society that can be solved through products or services. Entrepreneurs observe daily life to understand customer needs and market demands. Technology helps discover new opportunities in areas such as online education, e-commerce, and digital services. Successful entrepreneurs focus on solving real-world problems through innovative ideas.

Areas of Digital Business Opportunities in Pakistan

Agriculture

Technology can provide digital solutions for farmers, such as online farming services and information systems.

Healthcare

Digital services can help improve healthcare access and provide better solutions for patients.

Education

Online learning platforms provide opportunities to deliver education through digital technology.

Example

An entrepreneur creates an online learning platform that helps students access educational resources from anywhere.

Q. How does technology help entrepreneurs solve real-world problems? Explain the importance of recognizing market needs and customer demands.

Solving Real-World Problems Through Technology

Technology helps entrepreneurs solve real-world problems in faster and more effective ways. It allows people to create digital solutions for problems in different fields such as education, healthcare, agriculture, and business. Entrepreneurs use technology creatively to develop innovative products and services that improve people's daily lives.

Examples of Technology-Based Solutions

Education

Online learning platforms help students study from home and access educational resources easily.

Agriculture

Mobile applications help farmers improve crop production by providing useful information and services.

Business

Digital payment systems make financial transactions easier and safer.

Example

An entrepreneur develops a mobile app that helps farmers check weather information and improve farming decisions.

Recognizing Market Needs and Customer Demands

Recognizing market needs and customer demands means understanding what people need and the problems they face. Entrepreneurs study customer behavior, preferences, and market trends to create better products and services. They use surveys, customer feedback, and online data to identify gaps in the market. Understanding customer needs helps businesses provide useful solutions, increase customer satisfaction, and achieve success.

Importance of Understanding Customer Needs

Better Products and Services

Entrepreneurs can design products and services according to customer requirements.

Customer Satisfaction

Meeting customer needs improves customer trust and satisfaction.

Successful Business Ideas

Analyzing online trends and user feedback helps create successful business ideas in the digital economy.

Example

An online store studies customer reviews and feedback to improve its products and provide better services.

Q. Explain the role of digital platforms in entrepreneurship, including social media, e-commerce platforms, freelancing, remote work, and planning a small digital business.

Digital Platforms for Entrepreneurship using Social Media for Business Promotion

Digital platforms provide entrepreneurs with tools to start, manage, and grow their businesses online. These platforms include social media, e-commerce websites, and freelancing marketplaces. Social media helps in promoting products and reaching a large audience quickly. E-commerce platforms allow the buying and selling of goods without physical shops. Freelancing websites provide opportunities to offer skills and services globally, making entrepreneurship easier and more accessible.

E-commerce Platforms and Online Marketplaces

E-commerce platforms and online marketplaces allow businesses to sell products and services over the internet. They connect sellers with customers without the need for a physical store. These platforms make buying and selling easier, faster, and more accessible to a wider audience. Examples include websites and apps where users can browse products, compare prices, and place orders online. They play an important role in supporting digital entrepreneurship by reducing costs and expanding market reach.

Freelancing and Remote Work Opportunities

Freelancing and remote work allow individuals to offer their skills and services to clients through online platforms. Freelancers can work in areas such as graphic design, writing, programming, and digital marketing. Remote work enables people to work for companies from home or any location with an internet connection. These opportunities help students and professionals earn income independently. They are an important part of digital entrepreneurship as they provide flexibility and global access to job markets.

Planning a Small Digital Business

Planning a small digital business involves organizing ideas into a clear and workable plan. Entrepreneurs first identify a product or service that meets customer needs. They then decide on the target audience, pricing, and method of delivery using digital platforms. A basic budget is prepared to manage costs and expected income. Proper planning helps ensure the business is practical, organized, and more likely to succeed in the digital market.

Q. Explain Basic business planning concepts like budgeting, teamwork, innovation, and emerging technologies in digital entrepreneurship.

Basic Business Planning Concepts

Basic business planning involves setting clear goals for what a business wants to achieve. It includes identifying a product or service, understanding the target market, and deciding how to deliver value to customers. Entrepreneurs also plan resources such as time, money, and skills needed to run the business. A simple business plan helps organize ideas and provides direction for starting and growing a successful digital business.

Budgeting and Resource Management

Budgeting and resource management involve planning how money, time, and other resources will be used in a business.

A budget helps entrepreneurs estimate costs, set prices, and manage income and expenses properly. Proper resource management ensures that materials, skills, and tools are used efficiently without waste. In digital businesses, good budgeting and resource planning help maintain profitability and support long-term success.

Short Question

What is Budgeting and resource management in entrepreneurship?

Teamwork and Communication in Startups

Teamwork and communication are important for the success of startups and small digital businesses.

Team members work together by sharing ideas, responsibilities, and skills to achieve common goals. Effective communication reduces misunderstandings and improves decision-making. Startups use meetings, messaging apps, and online tools to maintain smooth workflow.

Strong teamwork and communication increase productivity and help businesses grow successfully.

Innovation and Future Opportunities

Innovation means creating new and improved ideas, products, or services to solve problems in better ways.

In digital entrepreneurship, innovation helps businesses grow and remain competitive. Technologies such as Artificial Intelligence, mobile apps, and online platforms are creating new opportunities and career paths for young entrepreneurs.

Short Question

What is Innovation?

By adopting innovation, individuals can build successful and future-ready digital businesses.

Example

A business creates a mobile application that provides a new and easier way for customers to access services.

Emerging Technologies and Entrepreneurship

Emerging technologies such as artificial intelligence, cloud computing, blockchain, and mobile applications are changing the field of entrepreneurship. These technologies help entrepreneurs create smarter, faster, and more efficient business solutions. They reduce costs, improve productivity, and allow businesses to reach customers globally through digital platforms.

Startups use these technologies to develop innovative products and services according to modern customer needs.

Q. Describe the role of AI, mobile apps, and digital services in modern business. Also explain different career opportunities in technology entrepreneurship.

Role of AI, Apps, and Digital Services in Business

Artificial Intelligence (AI), mobile apps, and digital services play an important role in modern business growth.

Artificial Intelligence (AI)

AI helps entrepreneurs analyze data, understand customer behavior, and improve decision-making.

Mobile Applications

Mobile apps help businesses reach customers, sell products, and provide services quickly.

Digital Services

Digital services such as online payments, cloud storage, and marketing tools improve efficiency and reduce costs. Together, these technologies support innovation and make businesses more competitive in the digital economy.

Career Pathways in Technology Entrepreneurship

Technology entrepreneurship provides different career opportunities for students in the digital age. Students can start their own digital businesses or work in technology-related fields. Many new career paths are growing because of digital technology.

Startup Founder

Individuals can create and launch their own digital businesses by developing new ideas and solutions.

Freelancing

People can work as freelancers in fields such as programming, graphic design, and digital marketing.

App Development

Students can build mobile applications and provide digital solutions.

E-commerce Management

Individuals can manage online stores and digital selling platforms.

Online Consultancy

Technology experts can provide online advice and services to businesses.

Innovators

Students can create new digital solutions to solve real-world problems.

? DO YOU KNOW?

- Most failed startups do not have a clear plan.

? DO YOU KNOW?

- AI tools can now design, write, and even help run businesses.



Additional Multiple Choice Questions

- Digital entrepreneurship is the use of technology and online platforms to:
 - Create, manage, and grow business ideas
 - Repair computers
 - Build computer networks
 - Install software
- Which of the following is a characteristic of successful entrepreneurs?
 - Carelessness
 - Creativity
 - Laziness
 - Hesitation
- Entrepreneurship in Pakistan is growing due to increased access to the:
 - Internet and mobile technology
 - Printed books
 - Television only
 - Newspapers only
- Identifying business opportunities means finding problems in society that can be solved through:
 - Products or services
 - Games only
 - Advertisements only
 - Social media posts
- Budgeting and resource management involve planning how _____ will be used in a business.
 - Computers and networks
 - Money, time, and other resources
 - Buildings only
 - Customers only
- Innovation means creating new and improved:
 - Buildings
 - Machines only
 - Ideas, products, or services
 - Documents
- Which emerging technology helps entrepreneurs analyze data, understand customer behavior, and improve decision-making?
 - Blockchain
 - Mobile applications
 - Cloud Computing
 - Artificial Intelligence (AI)
- Which digital service improves efficiency and reduces costs?
 - Online payments
 - Fax machines
 - Printed notices
 - Landline phones
- Which of the following is a career pathway in technology entrepreneurship?
 - Startup Founder
 - Bus Driver
 - Carpenter
 - Electrician
- Why is teamwork and communication important in startups?
 - They reduce internet usage
 - They increase productivity and help businesses grow successfully.
 - They increase paperwork
 - They replace innovation.

Answers:

- | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|---|
| 1 | A | 2 | B | 3 | A | 4 | A | 5 | B | 6 | C | 7 | D | 8 | A | 9 | A | 10 | C |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|---|

9.5 Ethical, Legal, and Environmental Impacts of Computing

Q. Explain the ethical, legal, and environmental impacts of computing. Discuss the importance of ethical use of technology.

Ethical, Legal, and Environmental Impacts of Computing

Ethical use means making fair and responsible choices while using digital tools. Legal use means following laws related to technology. Environmental impact includes energy consumption, electronic waste, and other effects on nature. Computing affects many areas of daily life. Technology can have ethical or unethical effects, legal or illegal consequences, and environmental impacts. Understanding these impacts helps users make responsible decisions while using computing resources.

Ethical Use of Technology

Ethical use of technology means using digital tools responsibly and avoiding actions that can harm others.

It includes respecting privacy, fairness, and proper handling of information. Following ethical guidelines helps maintain trust and safety online. Technology decisions should consider their effects on people, organizations, and society.

Responsible use of digital tools creates a safe and fair digital environment.

Short Question

What is ethical use of technology?

Respecting Intellectual Property and Data Ownership

Intellectual property refers to creative work such as software, music, videos, or written content. Data ownership refers to the right of a person or organization to control their personal information. Respecting these rights means avoiding copying, sharing, or using someone's work without permission.

Personal and sensitive information should be protected and not misused. Respecting intellectual property and data ownership promotes fairness and protects creators and users.

Understanding Consequences of Unethical Digital Behavior

Unethical digital behavior includes actions such as hacking, spreading false information, and cyberbullying. These actions can harm people, damage reputations, and cause legal problems. Even small online actions can create serious effects.

Understanding the consequences of unethical behavior encourages responsible digital activities. Following ethical standards helps create a safer and more trustworthy online environment.

? DO YOU KNOW?

- Copying online content without permission can violate both copyright laws and digital ethics.

Exo 0.7 Explain the legal aspects of computing by discussing international frameworks like GDPR and cybercrime laws and data protection policies in Pakistan. How do these laws protect digital information?

Legal Aspects and Data Privacy Laws

Legal aspects of computing refer to the rules and regulations that govern the use of technology and digital information.

Cybercrime refers to illegal activities performed using computers, networks, or the internet. Examples of cybercrime include hacking, identity theft, and online fraud.

Data privacy laws ensure that personal and sensitive information is collected, stored, and shared responsibly.

These laws protect individuals, organizations, and society from misuse of data and technology. Understanding legal rules helps prevent legal problems and promotes safe digital practices. Following legal frameworks also builds trust in online systems and services.

Short Question

What are Legal aspects and Data Privacy Laws of computing?

International Frameworks (GDPR)

The General Data Protection Regulation (GDPR) is a law of the European Union that protects personal data. It provides rules for organizations about collecting, storing, and using personal information. GDPR requires transparency, user consent, and the right to access or delete personal data.

Many countries and companies follow similar data privacy standards to protect information globally. These frameworks help prevent misuse of personal data and promote accountability.

Short Question

What is GDPR?

Cybercrime Laws and Data Protection Policies in Pakistan

Pakistan has laws to prevent cybercrime and protect digital information. The Prevention of Electronic Crimes Act (PECA) 2016 is the main law in Pakistan that deals with cybercrime. It protects individuals, organizations, and the state from illegal activities performed using computers, mobile devices, and the internet. These laws cover activities such as hacking, identity theft, online fraud, and unauthorized access to data. Organizations must follow data protection policies to keep sensitive information secure, and legal penalties are applied for violations.

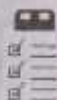
How These Laws Protect Digital Information

These laws protect digital information in many ways.

- They protect personal and sensitive information from misuse.
- They ensure that organizations collect, store, and share data responsibly.
- They give individuals greater control over their personal data.
- They discourage cybercrime by applying legal penalties.
- They help build trust in digital systems and online services.

Short Question

Describe importance of Cybercrime Laws? / How do cybercrime laws protect digital information?



CLASS ACTIVITY

Students list cybercrimes covered by PECA through a guided worksheet.

Sol:

S.No.	Cybercrime Covered by PECA
1.	Unauthorized access to computer systems (Hacking)
2.	Unauthorized copying or theft of data
3.	Cyberstalking and online harassment
4.	Identity theft and fake online identity
5.	Online financial fraud and scams
6.	Spreading malware or computer viruses
7.	Cyber terrorism
8.	Sending offensive or illegal online content
9.	Electronic forgery and fake digital documents
10.	Child exploitation through digital platforms

Learning Outcome:

Students will identify different cybercrimes covered under the Prevention of Electronic Crimes Act (PECA) and understand the importance of responsible and lawful use of technology.

Ex.Q.8. Discuss the environmental and social impacts of computing. Explain how e-waste management and sustainable computing practices can reduce harm to the environment, and describe the role of technology in cultural and societal change.

Environmental and Social Impacts

Computing affects the environment and society in many ways. Technology consumes energy, produces electronic waste, and can contribute to pollution. At the same time, technology affects social behavior, communication, and culture. Understanding environmental and social impacts helps promote responsible use of digital tools. Sustainable practices and awareness of digital effects help maintain a balance between technology, nature, and communities.

Example:

Using energy-efficient computers reduces electricity consumption and helps protect the environment.

E-waste Management and Sustainable Computing

Electronic waste (e-waste) is produced when electronic devices are discarded or replaced. Improper disposal of e-waste can damage the environment and harm human health. Sustainable computing focuses on reducing, reusing, and recycling electronic devices in a responsible way. Using energy-efficient devices and following environmentally friendly practices reduce the negative effects of technology. Proper e-waste management helps preserve resources and minimizes pollution.

Example

Recycling old computers and mobile phones instead of throwing them away helps reduce e-waste.

The Role of Technology in Cultural and Societal Change

Technology changes the way people communicate, work, and access information. Social media, digital learning, and online services have a strong impact on culture and daily life. Technology improves areas such as education, healthcare, and business by making services faster and easier.

However, technology can also create challenges such as the digital divide and loss of privacy. Understanding these social impacts helps people use technology responsibly in communities.



Additional Multiple Choice Questions

1. **Ethical use of technology means using digital tools:**
A) Responsibly B) Quickly C) Secretly D) Automatically
2. **Intellectual property refers to creative work such as:**
A) Roads and buildings B) Software, music, videos, or written content
C) Mobile networks D) Internet cables
3. **Data ownership refers to the right of a person or organization to:**
A) Sell computers B) Design websites
C) Control their personal information D) Build networks
4. **Which of the following is an example of unethical digital behavior?**
A) Using licensed software B) Respecting privacy
C) Protecting personal information D) Cyberbullying
5. **The General Data Protection Regulation (GDPR) is a law of the:**
A) Pakistan B) United States C) European Union D) China
6. **The Prevention of Electronic Crimes Act (PECA) 2016 is the main law in Pakistan that deals with:**
A) Environmental protection B) Cybercrime
C) Road safety D) Education
7. **Electronic waste (e-waste) is produced when electronic devices are:**
A) Purchased B) Repaired C) Upgraded D) Discarded or replaced
8. **Sustainable computing focuses on:**
A) Increasing electricity use B) Buying new devices regularly
C) Reducing, reusing, and recycling electronic devices D) Storing more data
9. **Which of the following is an example of sustainable computing?**
A) Throwing old computers into garbage B) Recycling old computers and mobile phones
C) Burning electronic waste D) Using copied software
10. **Technology improves areas such as education, healthcare, and business by:**
A) Increasing pollution B) Making services faster and easier
C) Reducing communication D) Replacing all human workers

Answers:

1	A	2	B	3	C	4	D	5	C	6	B	7	D	8	C	9	B	10	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	----	---

TEXTBOOK EXERCISE (SOLVED)

MULTIPLE CHOICE QUESTIONS

- The following helps keep online accounts secure:
(a) Weak passwords (b) Strong passwords (c) Sharing passwords (d) Simple passwords
- The main danger of downloading unknown software is:
(a) Faster browsing (b) Getting rewards (c) Malware infection (d) Extra storage
- The tool that adds an extra layer of login security is:
(a) Screensaver (b) Two-Factor Authentication (c) Wallpaper (d) Search engine
- The cyber threat that tricks users into giving personal information is:
(a) Phishing (b) Antivirus (c) Encryption (d) Backup
- The purpose of a firewall is to:
(a) Delete files (b) Block harmful network traffic (c) Play games (d) Slow down the computer
- Encryption is used to:
(a) Delete data (b) Make data readable to everyone
(c) Convert data into a secure form (d) Upload data automatically
- A commonly used platform for online collaboration is:
(a) Paint (b) Google Workspace (c) Notepad (d) VLC Player
- Digital etiquette means:
(a) Sharing all files freely (b) Using rude language online
(c) Safe and polite online behavior (d) Ignoring team members
- E-waste means:
(a) Old clothes (b) Electronic garbage (c) Raw materials (d) Food waste
- The international law that protects user privacy is:
(a) HTML (b) GDPR (c) CPU (d) LAN

Answers:

1	B	2	C	3	B	4	A	5	B	6	C	7	B	8	C	9	B	10	B
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	----	---



SHORT QUESTIONS

- What is the role of strong passwords in protecting data?

Ans: A strong password is a combination of letters, numbers, and symbols that helps protect accounts from hackers. It makes the password difficult for hackers to guess. A strong password is the first line of defense for protecting important files and online data. It improves the security of personal information.

- How can downloading suspicious software affect a computer?

Ans: Downloading software or files from unknown websites can harm your computer or steal your personal information. Some downloads contain viruses or spyware that secretly collect your information without permission. These harmful files can damage the system and create security risks. Software should be downloaded only from trusted websites.

- Why is it important to install software updates and security patches?

Ans: Software updates improve the security and performance of a computer system. They fix security gaps that hackers may use to attack a system. Updates also add new features and reduce the risk of malware infections and data theft. Regular updates keep computers reliable and protected from cyber threats.

- What are common types of cyber threats, such as phishing or ransomware?

Ans: Common cyber threats include viruses, phishing, ransomware, spyware, and DDoS attacks. A virus damages or deletes data, while phishing tricks users into sharing passwords or personal information. Ransomware locks data and demands payment to unlock it. Spyware secretly collects information, and DDoS attacks make online services unavailable.

5. **How does Two-Factor Authentication (2FA) improve online security?**

Ans: Two-Factor Authentication (2FA) is a security method that requires two forms of verification before allowing access to an account. After entering a password, the user must provide another verification, such as a code sent to a mobile phone or email. This extra security step makes it much harder for hackers to access the account. It provides better protection for personal data.

6. **Who is responsible for managing privacy and security settings on online platforms?**

Ans: Users are responsible for managing privacy and security settings on online platforms. They should control who can see their information and who can contact them. Users should allow only the permissions that are necessary for an app to work properly. Privacy and security settings should also be checked regularly.

7. **What is intellectual property, and why should it be respected in digital use?**

Ans: Intellectual property refers to creative work such as software, music, videos, or written content. It should be respected by avoiding copying, sharing, or using someone's work without permission. Respecting intellectual property promotes fairness and protects creators and users. It also supports the ethical use of technology.

8. **How does e-waste impact the environment, and what is sustainable computing?**

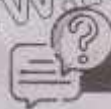
Ans: Electronic waste (e-waste) is produced when electronic devices are discarded or replaced. Improper disposal of e-waste can damage the environment and harm human health. Sustainable computing focuses on reducing, reusing, and recycling electronic devices in a responsible way. It helps preserve resources and minimizes pollution.

9. **Where do international data protection laws like GDPR apply?**

Ans: The General Data Protection Regulation (GDPR) is a law of the European Union that protects personal data. It provides rules for collecting, storing, and using personal information. Many countries and companies follow similar data privacy standards to protect information globally. These laws help prevent misuse of personal data and promote accountability.

10. **What is entrepreneurship?**

Ans: Entrepreneurship is the process of creating, managing, and growing a business. It involves identifying problems and providing useful products or services as solutions. Entrepreneurs use creativity and innovation to meet customer needs. Entrepreneurship creates business opportunities and supports economic growth.



LONG QUESTIONS

All QS are solved in chapter

1. Explain the importance of online safety and describe how strong passwords and safe browsing habits protect personal data.
2. Discuss the role of software updates and security patches in maintaining computer security, and explain the risks associated with outdated software.
3. Describe how privacy and security settings on online platforms can be managed. Explain why reading privacy policies is important for data protection.
4. Explain different types of cyber threats such as viruses, phishing, ransomware, spyware, and DDoS attacks. Discuss how these threats can affect both individuals and organizations.
5. Discuss security tools and techniques like Two-Factor Authentication (2FA), biometric verification, firewalls, intrusion detection systems (IDS), and antivirus software. Explain how each helps in protecting data.
6. Explain the concept of entrepreneurship and describe how digital technologies have created new opportunities for entrepreneurs. Include at least three examples of digital entrepreneurship.
7. Explain the legal aspects of computing by discussing international frameworks like GDPR and cybercrime laws and data protection policies in Pakistan. How do these laws protect digital information?
8. Discuss the environmental and social impacts of computing. Explain how e-waste management and sustainable computing practices can reduce harm to the environment, and describe the role of technology in cultural and societal change.

ADDITIONAL SHORT QUESTIONS

Online Safety

1. Why is online safety important?

Ans: Online safety is important because it prevents identity theft and fraud. It protects personal and school-related information from misuse. It reduces the risk of scams, viruses, and cyber threats. It also keeps online reputation and privacy safe.

2. Why should software be downloaded only from trusted sources?

Ans: Software should be downloaded only from trusted sources because unknown websites may contain harmful files. Trusted websites provide safer programs and reduce the risk of viruses and malware. This helps protect computer systems and personal data.

3. What is unsafe browsing?

Ans: Unsafe browsing means visiting fake websites or clicking unknown links without checking their reliability. It can lead to scams, identity theft, and malware infections. Users should avoid suspicious websites and links to stay safe online.

Software Maintenance and Updates

4. Why are software updates important?

Ans: Software updates are important because they improve the security and performance of computer systems. They fix errors, close security gaps, and add new features. Updates also reduce the risk of hacking, malware infections, and data theft.

5. What are the risks of outdated software?

Ans: Outdated software may contain security weaknesses that hackers can exploit. It can make the system slow, cause crashes, and create compatibility problems. It may also lead to data theft and malware infections.

Privacy and Security Settings

6. What are privacy and security settings?

Ans: Privacy and security settings help users control how their personal information is used and shared online. These settings are available in apps, websites, and online platforms. They protect information such as location, contacts, and browsing history from misuse.

7. What is a privacy policy?

Ans: A privacy policy explains how a website or app collects, stores, uses, and shares personal information. It helps users understand what data is collected and why it is collected. Users can make better decisions about sharing their information after reading the privacy policy.

Safe Online Collaboration

Digital Etiquette and Responsible Communication

8. What is digital etiquette?

Ans: Digital etiquette means communicating politely, respectfully, and responsibly in online environments. It includes using appropriate language and respecting others' opinions. Good digital etiquette creates a positive and professional online environment.

Cybersecurity Awareness

9. Why is cybersecurity awareness important?

Ans: Cybersecurity awareness is important because hackers use different tricks and harmful software to steal information or damage computer systems. It helps users recognize cyber threats and take preventive measures. It protects personal data, organizational information, and digital systems from attacks.

10. List different types of cyber threats.

Ans: There are different types of cyber threats such as viruses, phishing, ransomware, spyware, and DDoS attacks.

11. **What is a virus?**

Ans: A virus is a harmful program that spreads through infected files and can damage or delete data. It can enter a computer when a user opens an infected file or downloads unsafe software. Viruses can affect system performance and cause loss of important information.

12. **What is phishing?**

Ans: Phishing is a cyberattack that tricks people into sharing passwords or personal information through fake emails or websites. Attackers often create fake messages that look like trusted organizations. It can result in identity theft and loss of sensitive information.

13. **What is ransomware?**

Ans: Ransomware is a type of malware that locks data and demands payment to unlock it. It prevents users from accessing their important files. A ransomware attack can cause financial loss and damage computer systems.

14. **What is spyware?**

Ans: Spyware is a harmful program that secretly collects user information without permission. It can record usernames, passwords, and browsing activities. Spyware can affect user privacy and may cause data theft.

15. **What is a Distributed Denial of Service (DDoS) attack?**

Ans: A Distributed Denial of Service (DDoS) attack overloads a website with a large number of requests. It causes the website to slow down or stop working. This attack can interrupt online services and affect organizations.

Effects of Cyberattacks on Individuals and Organizations

16. **How do cyberattacks affect individuals and organizations?**

Ans: Cyberattacks can cause loss of personal data, passwords, and important files. They can also result in financial loss by stealing money or personal information. Cyberattacks can cause data breaches, financial losses, and disruption of business operations. Organizations may lose sensitive customer information and customer trust.

17. **What is a data breach?**

Ans: A data breach occurs when an organization loses sensitive data due to a cyberattack. This data may include customer information and other important records. Data breaches can harm an organization's security and reputation.

Security Tools and Techniques

18. **What are security tools and techniques?**

Ans: Security tools and techniques are used to protect computers and networks from online threats. These tools make it difficult for hackers and malicious software to access important information. They include authentication systems, firewalls, Intrusion Detection Systems (IDS), and antivirus programs. They detect and block harmful activities to keep data safe.

19. **What is biometric verification?**

Ans: Biometric verification is a security method that uses physical features to verify a user's identity. It uses fingerprints, face scans, or voice patterns for authentication. It provides strong protection for accounts and personal data.

20. **What is a firewall?**

Ans: A firewall acts as a barrier between a computer and the internet. It allows safe data to pass through and blocks harmful network traffic. It protects computers from unauthorized access and online threats.

21. **What is an Intrusion Detection System (IDS)?**

Ans: An Intrusion Detection System (IDS) monitors a network for suspicious activities. It detects possible security threats and alerts users about unusual network activity. It helps identify attacks and improves network security.

22. **What is antivirus software?**

Ans: Antivirus software scans files and removes viruses or malware before they can damage the system. Regular scanning helps keep computers and data safe from harmful software. It reduces the risk of malware infections.

Data Protection and Cryptography

23. What is data protection?

Ans: Data protection means keeping digital information safe from unauthorized access, loss, or damage. It ensures that only authorized people can access or use the data. Data protection helps maintain the security and privacy of digital information.

24. What are secure methods for transmitting and storing data?

Ans: Secure methods help protect data while it is stored or transferred over the Internet. These methods include encrypted connections, encrypted cloud storage, and regular backups. They prevent unauthorized access and protect data from loss or damage.

25. Why are regular backups important?

Ans: Regular backups help protect data from loss caused by system failure or cyberattacks. They allow users to restore important information when data is damaged or deleted. Backups improve data security and availability.

Troubleshooting and Preventive Measures

26. What is troubleshooting?

Ans: Troubleshooting is the process of finding the cause of a security problem and fixing it. It helps identify errors and apply suitable solutions. Troubleshooting improves system security and performance.

27. How can cyber threats be prevented?

Ans: Cyber threats can be prevented by installing firewalls, antivirus software, and anti-malware software. Users should regularly update software and change passwords. Harmful files should be removed, and important data should be restored from backups when needed.

Equity in Computing , Working Together Online, Tools and Platforms for Real-Time Collaboration

28. What is equity in computing and why is equity important in computing?

Ans: Equity in computing ensures that everyone, regardless of background or ability, can access and use digital resources equally. It provides equal opportunities to use technology and the Internet. Combining digital collaboration with fairness helps create inclusive and effective learning and working environments.

29. How does online teamwork help students?

Ans: Online teamwork improves problem-solving skills and builds interpersonal skills among students. It allows students from different locations to work together and share ideas. It also prepares students for modern workplaces where remote work is common.

30. What are real-time collaboration tools? Give examples

Ans: Real-time collaboration tools allow multiple users to work on the same project at the same time. These tools help users share documents, communicate, and conduct online meetings.

Examples: Google Workspace, Microsoft Teams, and Zoom

Designing for Equity and Accessibility

31. What is designing for equity and accessibility? Why is accessible design important?

Ans: Designing for equity and accessibility means creating technology that can be used by everyone, including people with different abilities and backgrounds. It provides equal opportunities to use technology and the Internet. Accessible design helps people with disabilities use technology easily. It also improves the overall usability of applications and websites.

Creating Inclusive Applications for Diverse Users

32. What are inclusive applications?

Ans: Inclusive applications are designed to fulfill the needs of different types of users. They include features that make applications easier to use for people with different abilities and backgrounds. They help create equal access to digital technology.

33. Why is innovation important in digital entrepreneurship?

Ans: Innovation is important because it helps in developing new products and services according to changing market needs. It allows entrepreneurs to create better solutions for customers. Innovation helps digital businesses grow and remain competitive.

Emerging Technologies and Entrepreneurship

34. Which emerging technologies are changing entrepreneurship?

Ans: Emerging technologies such as artificial intelligence, cloud computing, blockchain, and mobile applications are changing entrepreneurship. These technologies help create smarter and faster business solutions. They provide new opportunities for startups.

35. What is freelancing?

Ans: Freelancing allows people to work independently in fields such as programming, graphic design, and digital marketing. Freelancers provide online services to customers. It is an important career opportunity in technology entrepreneurship.

Ethical, Legal, and Environmental Impacts of Computing

36. What is the importance of ethical use of technology?

Ans: Ethical use of technology helps people make fair and responsible decisions while using digital tools. It protects privacy and promotes proper handling of information. Ethical practices create trust and safety among users, organizations, and society.

37. What is intellectual property?

Ans: Intellectual property refers to creative work such as software, music, videos, or written content. It gives creators the right to control and protect their work. Respecting intellectual property means avoiding copying or using someone's work without permission.

38. Give an example of unethical digital behavior.

Ans: Sharing fake information on social media is an example of unethical digital behavior. It can mislead people and damage someone's reputation. Such actions can create social and legal problems.

Legal Aspects and Data Privacy Laws

39. What is cybercrime? Why are data privacy laws important?

Ans: Cybercrime refers to illegal activities performed using computers, networks, or the internet. Examples of cybercrime include hacking, identity theft, and online fraud. Data privacy laws ensure that personal and sensitive information is collected, stored, and shared responsibly. These laws protect individuals and organizations from misuse of data.

40. What is PECA 2016?

Ans: The Prevention of Electronic Crimes Act (PECA) 2016 is the main law in Pakistan that deals with cybercrime. It protects individuals, organizations, and the state from illegal activities performed using computers, mobile devices, and the internet. It covers crimes such as hacking, identity theft, online fraud, and unauthorized access to data.

Environmental and Social Impacts of Computing

41. What are the environmental and social impacts of computing?

Ans: Computing affects the environment through energy consumption, electronic waste, and pollution. The use of electronic devices increases the demand for electricity and produces e-waste. Computing affects social behavior, communication, and culture. Technology helps people communicate, work, and access information easily.

42. What is e-waste? Why is e-waste management important?

Ans: Electronic waste (e-waste) is produced when electronic devices are discarded or replaced. Improper disposal of e-waste can damage the environment and harm human health. Proper management of e-waste helps reduce pollution. Recycling and reusing electronic devices help preserve resources and minimize pollution.

CONCEPTUAL SHORT QUESTIONS

- 1. A student receives an email asking for his password to verify his account. What should he do?**
Ans: The student should not share his password or click the link in the email. He should delete the email because it may be a phishing attack. Reporting the email and using trusted websites helps protect personal information.
- 2. A student uses the same password for all of his online accounts. Why is this not a safe practice?**
Ans: Using the same password for all accounts is not safe because if one account is hacked, other accounts can also be accessed. A different strong password should be used for each account. This improves online security.
- 3. A computer becomes slow after downloading software from an unknown website. What is the possible reason?**
Ans: The downloaded software may contain a virus or malware. Harmful software can damage the computer and steal personal information. Software should always be downloaded from trusted websites.
- 4. A company does not install software updates for several months. What problems can it face?**
Ans: Outdated software may contain security weaknesses that hackers can exploit. It also increases the risk of malware infections and data theft. Regular updates help keep systems secure and reliable.
- 5. A student shares his home address and phone number with strangers on social media. Why is this unsafe?**
Ans: Sharing personal information with strangers can lead to identity theft, fraud, or online harassment. Personal information should only be shared with trusted people. Privacy settings should also be managed carefully.
- 6. A startup team is working on a project, but members are not communicating properly. How can this problem be solved?**
Ans: Team members should communicate clearly and share their ideas regularly. They should assign responsibilities and work together to achieve common goals. Good communication improves teamwork and productivity.
- 7. An online store uses Artificial Intelligence (AI) to recommend products to customers. How does AI help the business?**
Ans: AI analyzes customer data and understands customer behavior. It helps entrepreneurs make better decisions and recommend suitable products. This improves customer satisfaction and business growth.
- 8. A school stores student records in encrypted cloud storage. Why is encryption important?**
Ans: Encryption converts readable data into coded text so that unauthorized people cannot read it. It protects information during storage and transmission. This helps keep digital information secure.
- 9. A young entrepreneur wants to sell handmade products across Pakistan without opening a physical shop. Which digital platform can help and why?**
Ans: The entrepreneur can use an e-commerce platform to sell products online. It allows businesses to reach more customers and manage sales through the internet. This reduces costs and increases business opportunities.
- 10. After completing a group project, students discuss what they did well and what they can improve. Why is this discussion important?**
Ans: This discussion is called reflection. It helps students identify their strengths and weaknesses and learn from their experience. Reflection improves teamwork and helps achieve better results in future projects.

TEST YOUR SKILLS

Total Marks: 40

Time: 1:30 Hour

8 x 1 = 8

Q.1 MULTIPLE CHOICE QUESTIONS

1. Digital etiquette means communicating:
(a) Quickly and secretly (b) Politely, respectfully, and responsibly
(c) Only through social media (d) Without following any rules
2. The main danger of downloading unknown software is:
(a) Faster browsing (b) Getting rewards (c) Malware infection (d) Extra storage
3. The tool that adds an extra layer of login security is:
(a) Screensaver (b) Two-Factor Authentication (c) Wallpaper (d) Search engine
4. Encryption is the process of converting readable data into:
(a) Printed text (b) Coded text (c) Digital images (d) Backup files
5. A commonly used platform for online collaboration is:
(a) Paint (b) Google Workspace (c) Notepad (d) VLC Player
6. E-waste means:
(a) Old clothes (b) Electronic garbage (c) Raw materials (d) Food waste
7. The international law that protects user privacy is:
(a) HTML (b) GDPR (c) CPU (d) LAN
8. Which of the following is a characteristic of successful entrepreneurs?
(a) Carelessness (b) Creativity (c) Laziness (d) Hesitation

Q.2 SHORT QUESTIONS:

Note: Attempt any 8 short questions

8 x 2 = 16

- i. Describe two characteristics of successful entrepreneur.
- ii. What is a privacy policy?
- iii. How Cyber attacks Affect Individuals and Organizations?
- iv. How can downloading suspicious software affect a computer?
- v. Why is it important to install software updates and security patches?
- vi. How does Two-Factor Authentication (2FA) improve online security?
- vii. What is a Distributed Denial of Service (DDoS) attack?
- viii. What is Cryptography in data protection?
- ix. How does e-waste impact the environment, and what is sustainable computing?
- x. A company does not install software updates for several months. What problems can it face?

LONG QUESTIONS:

Note: Attempt any 2 long questions

2 x 8 = 16

3. Explain different types of cyber threats such as viruses, phishing, ransomware, spyware, and DDoS attacks. Discuss how these threats can affect both individuals and organizations.
4. Explain the concept of entrepreneurship and describe how digital technologies have created new opportunities for entrepreneurs. Include at least three examples of digital entrepreneurship.
5. Discuss the environmental and social impacts of computing. Explain how e-waste management and sustainable computing practices can reduce harm to the environment, and describe the role of technology in cultural and societal change.