

scholareye.xyz



CLASS 9 | COMPUTER SCIENCE AND ENTREPRENEURSHIP

CHAPTER 11

Ethical, Social, And Legal Concerns in Computer Usage

Complete Exercise Solutions

MCQs with highlighted answers and explanations, short and long questions

15 MCQs

21 Short Questions

8 Long Questions

EXERCISE

Multiple Choice Questions (MCQs)

1

Why is it important to use computers safely and responsibly?

a) To ensure we can use them more frequently

b) To protect our personal information and make wise choices about hardware and software



c) To make the computer run faster

d) To avoid paying for software

Explanation: Using computers safely and responsibly is crucial to safeguarding your private data from cyber threats and ensuring that your hardware and software choices are secure, legitimate, and effective for your needs.

2

What does "responsible computer usage" include?

- a) Choosing the most expensive hardware
- b) Sharing your passwords with friends
- c) **Being cautious about what you share online and protecting yourself and others** 
- d) Ignoring software updates

Explanation: Responsible usage is about digital citizenship. It means being mindful of your digital footprint, respecting others' privacy, and taking active steps to protect yourself and others from online harm.

3

What should you check to ensure hardware and software compatibility?

a) The color of the hardware

b) The system requirements on software packages and match them with your computer's specifications



c) The price of the hardware

d) The brand of the hardware

Explanation: Before installing software, you must check its minimum system requirements (like RAM, processor speed, and OS version) to ensure your computer's hardware can actually support and run it smoothly.

4

Why is it important to use strong, unique passwords?

- a) To make your accounts easy to hack
- b) To help others guess your password
- c) **To make it harder for someone to guess your password and access your accounts**
- d) To avoid installing software updates



Explanation: Strong and unique passwords prevent hackers from using brute-force attacks or credential stuffing (where a leaked password from one site is tried on another) to gain unauthorized access to your accounts.

5

What is one reason to avoid clicking on unknown links or downloading files from untrusted sources?

- a) They might contain helpful software
- b) They might contain malware that can harm your device or steal your information** 
- c) They are usually cheaper
- d) They help your device run faster

Explanation: Untrusted links and downloads are primary vectors for malware, viruses, ransomware, and phishing scams designed to compromise your device and steal sensitive data.

6

What does Two-Factor Authentication (2FA) do?

- a) It makes your password easier to guess
- b) It adds an extra layer of security by requiring a second form of verification** 
- c) It removes the need for a password
- d) It reduces the need for software updates

Explanation: 2FA significantly enhances security. Even if a hacker steals your password, they cannot access your account without the second verification factor (like an OTP sent to your phone or a fingerprint scan).

7

Why should you be cautious when using public Wi-Fi for sensitive transactions?

- a) Public Wi-Fi is usually faster
- b) Public Wi-Fi networks are often less secure** 
- c) Public Wi-Fi is free
- d) Public Wi-Fi always provides encryption

Explanation: Public Wi-Fi networks are often unencrypted, making it easy for cybercriminals on the same network to intercept your data (man-in-the-middle attacks) and steal passwords or financial information.

8

What is an important aspect of responsible use of social media?

- a) Sharing personal information like your home address
- b) Posting photos without considering privacy settings
- c) **Being respectful and avoiding sharing sensitive information publicly** 
- d) Ignoring privacy settings

Explanation: Responsible social media use involves treating others with respect (avoiding cyberbullying) and protecting your own privacy by not oversharing sensitive personal information.

9

What should you do if you receive an email from an unknown sender asking for personal information?

- a) Provide the information requested
- b) Forward the email to your friends
- c) Ignore or delete the email**
- d) Open the email and click on any links



Explanation: This is a classic phishing attempt. You should never provide personal information, click links, or forward it. The safest action is to ignore and delete it, or report it as spam.

10

Why is it important to regularly review your account activity?

- a) To update your contact information
- b) To look for unusual activity and ensure your accounts are secure** 
- c) To check the number of friends you have
- d) To download new applications

Explanation: Regularly reviewing account activity helps you detect unauthorized access, fraudulent transactions, or suspicious logins early, allowing you to secure your account before major damage occurs.

11

What is the purpose of privacy settings on digital platforms?

- a) To make your posts public
- b) To control who can see your information and interact with you online** 
- c) To increase the number of followers
- d) To automatically share your information

Explanation: Privacy settings give users control over their digital footprint, allowing them to decide who can view their personal information, posts, and profile details.

12 What should you do to ensure data security?

- a) Use the same password for all accounts
- b) Share your passwords with friends
- c) Use strong, unique passwords and enable two-factor authentication** 
- d) Avoid using any security measures

Explanation: Using strong, unique passwords for every account, combined with enabling 2FA, is the most effective standard practice for securing your personal data against unauthorized access.

13 What is a key aspect of data ethics?

- a) Using data in any way you like
- b) Transparency, respect for privacy, and accountability in data usage** 
- c) Collecting as much data as possible
- d) Ignoring data security

Explanation: Data ethics revolves around doing what is morally right with data. This includes being transparent about data collection, respecting user privacy, and being accountable for how data is handled.

14 What is software piracy?

- a) Sharing software legally with friends
- b) The illegal copying, distribution, or use of software** 
- c) Buying software from an official source
- d) Updating software regularly

Explanation: Software piracy is the unauthorized reproduction, distribution, or use of copyrighted software, which is a serious legal and ethical violation.

15

How can you verify the credibility of information found online?

- a) By checking the number of ads on the website
- b) By using multiple reputable sources and checking the author's credentials** 
- c) By looking at the website's design
- d) By the website's popularity

Explanation: To ensure information is credible, you should cross-reference it with multiple reliable sources, check the author's expertise, and evaluate the website's domain (e.g., .edu, .gov) and publication date.

Short Questions

1

What is the importance of using computers safely and responsibly?

Using computers safely and responsibly is vital to protect personal and financial information from cyber threats (like malware and phishing), maintain privacy, ensure the longevity of hardware, and foster a respectful and secure digital environment for everyone.

2

How does choosing the right hardware and software affect your computer usage?

Choosing the right hardware and software ensures compatibility, optimal performance, and efficiency. It prevents system crashes, allows you to run necessary applications smoothly, and provides a better overall user experience tailored to your specific needs.

3**Why is it important to use antivirus software on your computer?**

Antivirus software is crucial because it detects, blocks, and removes malicious software (viruses, ransomware, spyware). It acts as a protective shield, preventing data loss, system damage, and unauthorized access to your personal information.

4**What are some examples of good practices when selecting hardware and software?**

Good practices include: checking system requirements for compatibility, reading reviews and comparing specifications, purchasing from official and reputable sources, ensuring the software is licensed and legitimate, and considering future upgrade needs.

5

How can choosing compatible hardware and software enhance your computer experience?

When hardware and software are compatible, the system runs smoothly without lagging or crashing. It allows you to utilize all the features of the software, increases productivity, reduces troubleshooting time, and extends the lifespan of your device.

6

Why should you create strong, unique passwords for your accounts?

Strong, unique passwords are essential to prevent credential stuffing and brute-force attacks. If one account is compromised, using unique passwords ensures that hackers cannot access your other accounts, thereby protecting your overall digital identity.

7

What is the purpose of regular software updates?

Regular software updates patch security vulnerabilities, fix bugs, improve system stability, and sometimes introduce new features. They are critical for defending against evolving cyber threats and ensuring optimal performance.

8

How can you protect yourself from harmful links and downloads?

You can protect yourself by never clicking on links or downloading attachments from unknown senders. Hover over links to check the URL, use reputable antivirus software, keep your browser updated, and avoid downloading files from untrusted websites.

9

What is Two-Factor Authentication (2FA), and why is it useful?

2FA is a security process that requires two different forms of identification to access an account (e.g., a password and a code sent to your phone). It is useful because it adds a second layer of security, making it significantly harder for hackers to gain access even if they steal your password.

10

Why is it a good idea to avoid using public Wi-Fi for sensitive transactions?

Public Wi-Fi networks are often unsecured and unencrypted. Hackers on the same network can easily intercept your data, including login credentials and financial information, making it unsafe for sensitive transactions like online banking.

11**How can you verify if an email or message is a scam?**

You can verify a scam by checking the sender's email address for inconsistencies, looking for spelling and grammar errors, being wary of urgent or threatening language, and noticing if they ask for personal information or direct you to click suspicious links.

12**Why is it important to be careful about what you share on social media?**

Being careful is important to protect your privacy, prevent identity theft, maintain your professional reputation, and avoid physical security risks. Oversharing personal details can be exploited by cybercriminals or malicious individuals.

13**What should you do if you receive an email from an unknown sender asking for personal information?**

You should never respond, provide the information, or click any links. Instead, mark the email as spam or phishing, report it to your email provider, and delete it immediately.

14**What is the purpose of privacy laws regarding your personal information?**

Privacy laws are designed to protect individuals by regulating how organizations collect, store, use, and share personal data. They give users rights over their information and mandate that companies handle data transparently and securely.

15

How do privacy laws protect you from unauthorized access to your data?

Privacy laws require organizations to implement strict security measures, obtain consent before collecting data, and notify users of data breaches. They also impose heavy penalties on companies that fail to protect user data from unauthorized access.

16

What is the difference between copyright, trademarks, and patents?

Copyright protects original creative works (like books, music, and art). **Trademarks** protect brand identifiers (like logos, names, and slogans). **Patents** protect new inventions, processes, or designs.

17

Why is it important to respect intellectual property rights?

Respecting intellectual property rights is important to encourage innovation and creativity, protect the livelihoods of creators and inventors, ensure ethical business practices, and avoid legal consequences.

18**What is software piracy, and why is it harmful?**

Software piracy is the illegal copying, distribution, or use of licensed software. It is harmful because it robs developers of revenue, discourages innovation, exposes users to malware (as pirated software is often infected), and provides no technical support or updates.

19**How can you identify reliable sources when researching online?**

You can identify reliable sources by checking the author's credentials, looking for reputable domain extensions (like .edu or .gov), verifying the publication date, checking for citations, and cross-referencing the information with other trusted sources.

20**What is one way to protect your privacy during online research?**

One effective way is to use a Virtual Private Network (VPN) or incognito mode to prevent your browsing history from being saved. You should also avoid logging into personal accounts while researching and clear your cookies regularly.

21**What are some signs that you might be developing an internet addiction?**

Signs include preoccupation with the internet, withdrawal symptoms when offline, losing track of time online, neglecting responsibilities (work, school, hygiene), and using the internet to escape from negative feelings.

Long Questions

1

Discuss the importance of responsible computer usage in today's digital world. Explain how selecting the right hardware and software can affect safety, efficiency, and compatibility in computer use.

Responsible Computer Usage: In today's interconnected digital world, responsible computer usage is paramount. It encompasses ethical behavior, digital safety, and respect for others. It is important because our personal, financial, and professional lives are deeply intertwined with technology. Irresponsible use can lead to data breaches, identity theft, cyberbullying, and the spread of misinformation.

Impact of Selecting the Right Hardware and Software:

- **Safety:** Choosing reputable software from official sources reduces the risk of malware and viruses. Similarly, hardware with built-in security features (like TPM chips) enhances data safety.
- **Efficiency:** Matching hardware specifications (e.g., RAM, CPU) to the demands of the software ensures smooth multitasking and faster processing. Using outdated

hardware with modern software leads to frustrating lag and decreased productivity.

- **Compatibility:** Ensuring software system requirements match the computer's specifications is crucial. Incompatible combinations result in crashes, driver conflicts, and the inability to run necessary applications. Proper selection guarantees a seamless and productive computing experience.

2

Describe the steps you should take to ensure the safe operation of digital platforms and devices.

To ensure safe operation, a multi-layered approach is required:

1. **Authentication:** Always use strong, unique passwords for every account and enable Two-Factor Authentication (2FA) wherever possible.
2. **System Maintenance:** Regularly update your operating system, browsers, and applications to patch security vulnerabilities. Install and regularly update reputable antivirus and anti-malware software.
3. **Safe Browsing:** Avoid clicking on unknown links or downloading attachments from untrusted sources. Be highly cautious when using public Wi-Fi; use a VPN if you

must conduct sensitive transactions.

- 4. Privacy Management:** Review and configure privacy settings on all social media and digital platforms to control who sees your information.
- 5. Data Backup:** Regularly back up important data to an external drive or a secure cloud service to prevent data loss in case of a ransomware attack or hardware failure.

3

Explain the concept of data ethics and its importance in handling personal and sensitive information. Discuss the principles of transparency, respect for privacy, and accountability.

Data Ethics refers to the moral principles and values that govern how data is collected, stored, shared, and used. It goes beyond legal compliance to ask what is *right* and *fair* regarding data handling.

- **Importance:** With the massive amounts of data being generated daily, ethical handling is crucial to maintain user trust, prevent discrimination, and protect vulnerable individuals from harm.
- **Transparency:** Organizations must be open about what data they collect, why they collect it, and how it will be used. Users should not be kept in the dark.

- **Respect for Privacy:** Individuals have the right to control their personal information. Data should only be collected with informed consent, and users should have the right to access, correct, or delete their data.
- **Accountability:** Organizations must take responsibility for the data they hold. If a data breach occurs or data is misused, the organization must be held accountable and face consequences.

4

Analyze the impact of privacy laws on protecting personal information in the digital age. How do laws like the Personal Data Protection Bill in Pakistan help safeguard user data?

Impact of Privacy Laws: Privacy laws (like GDPR in Europe) have revolutionized data protection by shifting the power dynamic back to the user. They mandate that companies obtain explicit consent, limit data collection to what is necessary, and impose heavy fines for violations.

The Personal Data Protection Bill in Pakistan: This bill is designed to regulate the processing of personal data in Pakistan. It helps safeguard user data by:

1. Requiring organizations to obtain consent before collecting personal data.

2. Establishing strict guidelines on how data can be stored and transferred across borders.
3. Granting citizens the right to access and correct their data.
4. Imposing penalties on organizations that fail to protect data or violate privacy rights, thereby forcing companies to prioritize cybersecurity.

5

Discuss the different types of intellectual property rights, including copyright, trademarks, and patents.

Intellectual Property (IP) rights are legal protections granted to creators and inventors for their creations.

- **Copyright:** Protects original works of authorship, including literary, dramatic, musical, and artistic works (e.g., books, songs, paintings, software code). It prevents others from copying or distributing the work without permission.
- **Trademarks:** Protects symbols, names, slogans, and logos used to identify and distinguish a company's products or services in the marketplace (e.g., the Nike swoosh or the Apple logo).
- **Patents:** Protects new inventions, processes, machines, or chemical compositions. A patent gives the inventor the

exclusive right to make, use, or sell the invention for a limited time (usually 20 years), encouraging innovation by allowing inventors to profit from their work.

6

Describe the ethical and legal responsibilities related to intellectual property rights. What are the consequences of violating these rights, such as through software piracy or unauthorized use of copyrighted material?

Ethical and Legal Responsibilities: Ethically, individuals and organizations must respect the hard work and creativity of others by not stealing or misusing their intellectual property. Legally, everyone must comply with copyright, patent, and trademark laws. This includes purchasing legitimate software licenses, citing sources properly, and not reproducing copyrighted material without permission.

Consequences of Violation:

- **Legal:** Violating IP rights can result in civil lawsuits, heavy financial penalties, and even criminal charges leading to imprisonment.
- **Software Piracy:** Using pirated software is not just illegal; it poses severe security risks. Pirated software often contains hidden malware and spyware. Furthermore, users receive no technical support or

security updates, leaving them highly vulnerable to cyberattacks. Ethically, it undermines the software industry, leading to higher prices for legitimate consumers and reduced funding for future innovation.

7

Outline effective techniques for conducting safe and credible online research. How can users evaluate the reliability of sources and avoid privacy risks during their research?

Techniques for Safe and Credible Research:

- 1. Evaluate Credibility:** Use the CRAAP test (Currency, Relevance, Authority, Accuracy, Purpose). Check the author's credentials, look for reputable domains (.edu, .gov, .org), and verify the publication date. Cross-reference information across multiple sources.
- 2. Avoid Privacy Risks:**
 - Use incognito or private browsing modes to prevent local data storage.
 - Use a VPN (Virtual Private Network) to encrypt your connection and mask your IP address.
 - Avoid logging into personal accounts (like Google or Facebook) while researching sensitive topics.
 - Never download files from untrusted websites. Look for HTTPS in the URL before entering any information.

- Use ad-blockers and tracker blockers to prevent websites from collecting browsing data.

8

Discuss the concept of internet addiction and its potential impact on individuals. How can recognizing the signs of addiction, setting time limits, and finding offline activities help promote balanced internet usage?

Internet Addiction: Internet addiction is a behavioral addiction characterized by excessive or poorly controlled preoccupations, urges, or behaviors regarding computer use and internet access that lead to impairment or distress.

Potential Impacts: It can severely affect an individual's physical health (eye strain, poor posture, sleep deprivation), mental health (anxiety, depression, social isolation), and professional/academic life (declining grades, job loss, neglect of responsibilities).

Promoting Balanced Usage:

- **Recognizing Signs:** Acknowledging the signs (preoccupation, withdrawal, lying about usage) is the first step toward recovery.
- **Setting Time Limits:** Using screen time tracking apps or setting strict schedules for internet usage helps break the cycle of endless scrolling.

- **Finding Offline Activities:** Replacing screen time with physical exercise, hobbies, face-to-face social interactions, and outdoor activities helps rewire the brain's reward system and provides a healthier outlet for stress.
- **Seeking Help:** In severe cases, cognitive-behavioral therapy (CBT) or support groups can be highly effective in treating internet addiction.



Thank You!

Think before you click.
Protect your data. Respect others' work.
Be a responsible digital citizen.

scholareye.xyz

Class 9 | Computer Science and Entrepreneurship | Chapter 11