

Class 9th Computer Science

Unit # 6

Impacts of Computing

Multiple Choice Questions Answers

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

Short Questions Answers

Q#1. Illustrate the responsible use of computer hardware by an individual.

Ans.Responsible use of computer hardware by an individual entails:

- Handling devices with care to prevent physical damage.
- Keeping hardware clean and dust-free to maintain optimal performance.
- Using devices in appropriate environments with proper ventilation and temperature control.
- Regularly backing up data to prevent loss in case of hardware failure.
- Installing and updating antivirus software to protect against malware and Security threats.

Q#2. What does appropriate software use entail?

Ans. Appropriate software use entails:

- Adhering to software licenses and copyrights.
- Using software for its intended purpose.
- Respecting terms of service and user agreements.
- Regularly updating software for security and performance.

- Avoiding piracy and using legitimate copies of software.

Q#3. How do you stay safe while conducting data searches online?

Ans. To stay safe while conducting data searches online:

- Use reputable search engines.
- Verify website credibility before sharing personal information.
- Check website security (look for HTTPS).
- Use privacy-focused search engines for sensitive searches.
- Avoid clicking on suspicious links or ads.
- Be cautious when downloading files or software.
- Use strong, unique passwords for accounts related to searches.
-

Q#4. Extract and enlist some key aspects of responsible social networking?

Ans. Key aspects of responsible social networking include:

- Protecting personal information and privacy settings.
- Being mindful of the content shared and its potential impact.
- Respecting others' privacy and intellectual property.
- Engaging in civil and respectful interactions.
- Verifying information before sharing or reposting. Reporting inappropriate or harmful content.
- Setting boundaries and managing screen time effectively.
- Being cautious of online relationships and interactions with strangers.

Q#5 Sketch the positive impacts of social networking in today's society?

Ans. Positive impacts of social networking in today's society:

- Enhanced communication and connectivity.
- Increased access to information and diverse perspectives.
- Facilitation of social movements and activism.
- Opportunities for professional networking and career advancement.
- Support for mental health and well-being through online communities.
- Platform for creative expression and collaboration.
- Bridge for maintaining relationships across distances. Amplification of voices and democratization of information.

Q#6 Relate fake news affecting our understanding of current events?

Ans. Fake news can distort our understanding of current events by spreading misinformation, manipulating public opinion, and undermining trust in credible sources. This misinformation can lead to confusion, polarization, and misguided decision-making, ultimately impacting societal perceptions and responses to important issues

Q#7 Summarize some of the adverse effects of social networking?

Ans. Adverse effects of social networking include:

- Increased risk of cyberbullying and harassment.
- Negative impact on mental health, including anxiety and depression.
- Reduced face-to-face social interactions and loneliness.
- Privacy concerns and data breaches.
- Spread of misinformation and fake news.
- Addiction and excessive screen time.
- Comparison and self-esteem issues due to curated online persons. Impact on productivity and academic performance.

Q#8 Interpret the dangers associated with the spread of fake news online?

Ans. The spread of fake news online poses significant dangers, including:

- Misinforming the public and distorting perceptions of reality.
- Undermining trust in credible sources and institutions.
- Fueling societal polarization and division.
- Manipulating public opinion and influencing political outcomes.
- Fostering confusion and hindering informed decision-making.
- Exacerbating social tensions and conflicts.
- Promoting distrust and skepticism in legitimate information sources.
- Increasing susceptibility to scams, misinformation, and propaganda.

Q#9 Examine the computing influence on personal privacy?

Ans. Computing has both positive and negative impacts on personal privacy:

Positive influences:

- Encryption and secure communication tools enhance privacy.
- Privacy-focused technologies allow individuals to control their data.
- Privacy settings on social media platforms enable users to manage their online presence.
- Anonymization techniques protect personal information in research and data analysis.

Negative influences:

- Data collection practices by companies and governments compromise privacy.
- Surveillance technologies invade personal privacy.
- Data breaches and cyber-attacks expose personal information to unauthorized parties.
- Algorithmic profiling and targeting erode privacy by analyzing and predicting individual behavior.

Q#10 Criticize about the role computing plays in shaping educational practices.?

Ans. Computing has revolutionized educational practices in many ways, but it's not without criticism:

Access and Equity: While computing offers vast educational resources, access to technology and the internet remains unequal, widening the digital divide.

Depersonalization: Over-reliance on technology can depersonalize learning experiences, reducing meaningful interactions between students and teachers.

Distraction: Computing devices can be a source of distraction, leading to reduced attention spans and academic performance.

Technological Dependence: Excessive reliance on computing can hinder critical thinking and problem-solving skills, as students may rely on technology for answers rather than developing their own solutions

Long Questions Answers

Q#1. Identify the precautions that need to be taken to ensure the physical safety of computer hardware?

Ans: Precautions:

- Wear the right clothes. Don't wear things like wool sweaters or loose jewelry when working with electronics.
- Always unplug computers and devices before opening them unless you're using an anti-static mat it keeps everything safe.
- Keep your workspace clean, tidy, and well-lit. Make it an excellent place to work.
- Look for broken parts. Tell your teacher if something needs to be corrected. Be gentle with computer parts. If something doesn't fit, don't force it. Ask for help.
- Use something like an anti-static wrist strap or touch something metal before touching computer parts.
- Read carefully about power supplies. Only open them if your teacher says it's okay.
- Check everything with the teacher before turning things on.
- Always put the covers back on after working on computers. Use the suitable screws and ask for more if needed.
- Keep all the screws when taking things apart. Please put them in containers by size to put things back together correctly.
- Computers shouldn't get hot. If they do, turn them off right away and tell the teacher.

Q#2. Judge the meaning of software legally and ethically?

Ans:

Legal Meaning of Software

1. Intellectual Property Protection

- **Copyright:** This legal right protects the expression of an idea, which in software translates to the source code and other creative elements. Copyright prevents unauthorized copying, modification, and distribution of the software.
- **Patents:** In some cases, software can also be protected by patents, which grant exclusive rights to an invention, including novel and non-obvious algorithms or processes implemented in the software.

2. Software Licenses

Software licenses are legal agreements that define the terms and conditions under which users can use, distribute, and modify software. These licenses vary widely, ranging from permissive open-source licenses to restrictive proprietary licenses. Understanding and adhering to these licenses is crucial for legal software use.

Ethical Meaning of Software

1. Respecting Intellectual Property Rights

- **Avoiding Piracy:** Unauthorized copying and distribution of software is not only illegal but also unethical, as it deprives creators of their rightful compensation.
- **Proper Licensing:** Using software within the bounds of its license agreement is essential. This includes obtaining appropriate licenses for commercial use or adhering to the terms of open-source licenses.

2. Responsible Development and Deployment

- **Avoiding Harm:** Software should be developed and deployed in a way that minimizes potential harm to users or society. This includes ensuring software safety, security, and reliability.
- **Protecting Privacy:** Software should be designed to respect user privacy, collecting and using data responsibly and transparently.
- **Accessibility:** Ethical software development strives to create software that is accessible to all users, including those with disabilities.

3. Professional Responsibility

- **Maintain Competence:** Staying up-to-date with the latest technologies and best practices to ensure the quality and safety of their work.
- **Act with Integrity:** Upholding ethical principles in their work, avoiding conflicts of interest and acting honestly.
- **Promote Ethical Practices:** Encouraging ethical behaviour within their organizations and the software industry as a whole.

Q#3. Express the ways, user can recognize and protect themselves from online cheats and phishing attempts?

Ans.

Educate Yourself:

- Stay informed about common phishing techniques and online scams. Understand how they work and the methods used by scammers to trick victims.
- Regularly read articles, blogs, and resources provided by reputable cyber security organizations to stay updated on the latest threats and trends.

Verify Sender Information:

- Always check the sender's email address or website URL carefully. Phishing emails often use slight variations of legitimate domain names or email addresses to deceive users.
- Look for spelling errors or unusual characters in domain names, as these are common red flags.

Think Before Clicking:

- Avoid clicking on links or downloading attachments from unknown or suspicious sources, especially in emails or messages.
- Hover your mouse over hyperlinks to preview the URL before clicking. If it looks suspicious or unfamiliar don't click on it.

Use Two-Factor Authentication (2FA):

- Enable two-factor authentication whenever possible, especially for sensitive accounts like emails, banking and social media. 2FA adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone.

Keep Software Updated:

- Ensure your operating system, antivirus software, web browsers, and other applications are regularly updated with the latest security patches.
- Vulnerabilities in outdated software can be exploited by cybercriminals.

Use Strong, Unique Passwords:

- Create strong passwords using a combination of letters, numbers, and- special characters. Avoid using easily guessable information such as birthdays or pet names.

- Use a different password for each online account to prevent a single breach from compromising multiple accounts.

Be Wary of Urgent Requests:

- Be cautious of emails, messages, or calls that create a sense of urgency or pressure you to act quickly.
- Scammers often use tactics like claiming your account will be suspended unless you provide personal information immediately.
- Take your time to verify the legitimacy of the request through independent means, such as contacting the organization directly using a verified phone number or visiting their official website.

Install Antivirus Software:

- Use reputable antivirus or antimalware software on your devices to detect and block malicious software, including phishing attempts.
 - Keep the antivirus software updated to ensure it can recognize the latest threats.
- Monitor Your Accounts Regularly:

Trust Your Instincts:

- If something feels off or too good to be true, it probably is. Trust your instincts and err on the side of caution.
- Don't hesitate to double-check with trusted sources or seek advice from cyber security experts if you're unsure about the legitimacy of communication of website.

Q#4.Comment on the key ways in which social networking platforms have revolutionized communication and connectivity in the digital age.Additionally,deduce the positive impacts of these changes on society?

Ans.

Ans: Social networking:

Social networking refers to the practice of using online platforms and websites to connect with other people, build relationships, share information, and engage in various forms of communication and interaction. These platforms are designed to facilitate the exchange of ideas, interests, and personal updates among users. Social networking has become an integral part of many people's lives, both for personal and professional purposes.

Some of the most popular social networking sites include Facebook, Twitter, Instagram, YouTube and WhatsApp.

Social networking platforms have become an integral part of modern life, providing opportunities for communication, information sharing, and entertainment. Social media

platforms can facilitate cyber bullying, where individuals are harassed, threatened, or humiliated online.

This can have severe psychological consequences for victims. Many social networks collect vast amounts of personal data, sometimes without Users' full awareness or consent.

This data can be misused or exposed in security breaches. Social media can spread false information rapidly, contributing to the dissemination of misinformation and conspiracy theories, which can have real-world consequences.

Positive impacts on society:

- The positive impacts of social networking on society in short:
- Enhanced communication and connectivity
- Access to diverse information and perspectives
- Networking and collaboration opportunities
- Community building and support
- Promotion of social causes and activism Business growth and innovation
- Cultural exchange and understanding
- Empowerment of individuals
- Educational opportunities
- Mental health support and awareness.

Q#5. Describe the risks associated with online gaming and social networking for children?

Ans.Online gaming and social networking can offer numerous benefits for children, including opportunities for learning, socialization, and entertainment. However, they also come with several risks that parents and guardians should be aware of:

1. Exposure to Inappropriate Content:

Children may encounter inappropriate content such as violence, explicit language, or graphic imagery while gaming or browsing social networking sites. This can have negative effects on their emotional and psychological development.

2. Online Predators:

Social networking platforms and online gaming communities can be targets for predators who seek to exploit children. Predators may use deceptive tactics to gain children's trust and engage in grooming behavior with the intention of sexual exploitation or manipulation.

3. Cyber bullying:

Online gaming and social networking can expose children to cyber bullying, where they may be subjected to harassment, intimidation, or exclusion by peers. Cyber bullying can have serious consequences on children's mental health and well-being.

4. Privacy and Data Security Concerns:

Children may not fully understand the importance of privacy settings and the risks associated with sharing personal information online. This leaves them vulnerable to privacy breaches, identity theft, and other forms of exploitation.

5. Addiction and Excessive Screen Time:

Excessive gaming or social networking can lead to addiction and unhealthy screen time habits, impacting children's physical health, academic performance, and social relationships. It can also contribute to sleep disturbances and behavioral problems.

6. Impact on Social Skills:

Spending too much time online may detract from face-to-face interactions and hinder the development of essential social skills such as empathy, communication, and conflict resolution.

7. Online Scams and Fraud:

Children may be susceptible to online scams, phishing attempts, or fraudulent schemes while gaming or engaging in social networking. They may unknowingly share sensitive information or fall victim to deceptive practices.

8. Exposure to Gambling and In-Game Purchases:

Some online games incorporate gambling-like mechanics or encourage in-game purchases, which can normalize risky behaviors and lead to financial consequences for children and their families.

9. Desensitization to Violence:

Exposure to violent content in online games and social media can desensitize children to real-world violence and lead to aggressive behavior or desensitization to the consequences of violence.

10. Distraction from Responsibilities:

Excessive engagement in online gaming or social networking can distract children from their schoolwork, chores, and other responsibilities, impacting their academic performance and overall productivity.

Q#06. Devise steps for governments and businesses in leveraging computing to drive economic growth and innovation?

Ans: Harnessing the power of computing can significantly drive economic growth and innovation for both governments and businesses. Here's a detailed guide outlining steps for governments and businesses to leverage computing effectively:

For Governments:

1. Invest in Digital Infrastructure:

Governments should prioritize investments in robust digital infrastructure, including high-speed internet access, data centers, and cloud computing services. This infrastructure forms the backbone of digital economies and enables businesses leverage computing effectively.

2. Promote Digital Literacy and Skills Development:

Governments should invest in programs to enhance digital literacy and equip citizens with the necessary skills for the digital workforce. This includes initiatives for training in coding, data analytics, cyber security, and other relevant fields.

3. Facilitate Research and Development (R&D):

Governments can support R&D initiatives in computing technologies through funding, grants, and partnerships with academic institutions and private sector organizations. This fosters innovation and drives the development of cutting-edge technologies.

4. Support Digital Transformation in Public Services:

Governments should lead by example in adopting digital technologies and modernizing public services. This includes digitizing government processes, implementing e-government solutions, and leveraging data analytics for evidence-based policymaking.

5. Encourage Collaboration and Partnerships:

Governments can facilitate collaboration between industry stakeholders, academia, and research institutions to foster innovation ecosystems. Public-private partnerships can accelerate technology adoption, drive research initiatives, and create synergies for economic growth.

For Businesses:

1. Embrace Cloud Computing and Data Analytics:

Businesses should leverage cloud computing services to access scalable computing resources and reduce infrastructure costs. Additionally, adopting data analytics technologies enables businesses to extract insights from large volumes of data, driving informed decision-making and innovation.

2. Invest in Research and Development:

Businesses should allocate resources for R&D efforts aimed at developing innovative products, services, and solutions powered by computing technologies. This may involve establishing dedicated R&D teams, partnering with research institutions, or participating in industry consortia.

3. Promote Digital Skills Development:

Businesses should invest in training programs to up skill their workforce in digital technologies and computing skills. This ensures that employees are equipped to leverage emerging technologies and drive innovation within the organization.

4. Collaborate with Start-ups and SMES:

Large enterprises can foster innovation by collaborating with start-ups and small to medium-sized enterprises (SMEs) in the technology ecosystem. This includes partnerships for technology development, joint ventures, and investment in promising start-ups.

5. Protect Intellectual Property Rights:

Businesses should prioritize the protection of intellectual property rights related to computing technologies, including patents, copyrights, and trade secrets. This safeguards their innovations and provides a competitive advantage in the market.

Q#07. Compare the impact of online platforms and algorithms on cultural diversity and the spread of global or local culture?

Ans: The impact of online platforms and algorithms on cultural diversity and the spread of global or local culture is complex and multifaceted. Here's a detailed comparison:

Impact on Cultural Diversity:

1. Online Platforms:

- Online platforms have the potential to both enhance and diminish cultural diversity. On one hand, they provide a space for diverse voices and communities to express themselves, share their cultures, and connect with others globally.
- Social media platforms, in particular, allow individuals to share their cultural practices, traditions, and languages with a worldwide audience, fostering cross-cultural understanding and appreciation.
- However, the dominance of a few major online platforms can also lead to homogenization and the marginalization of minority cultures. Popular platforms often prioritize content that appeals to the widest audience, potentially overshadowing niche cultural content.

2. Algorithms:

- Algorithms play a significant role in shaping the online experience by curating content based on user preferences, engagement patterns, and demographic data. While this can personalize the user experience, it also has implications for cultural diversity.
- Algorithms tend to prioritize content that aligns with users' existing preferences, leading to filter bubbles and echo chambers where users are exposed to a limited range of viewpoints and cultural perspectives.
- This can reinforce stereotypes, bias, and cultural hegemony, as content that deviates from the users' feeds.

Impact on the Spread of Global or Local Culture:

1. Online Platforms:

- Online platforms facilitate the spread of both global and local culture. Globalization has enabled the widespread dissemination of cultural products such as music, films, and literature through digital platforms, reaching audiences worldwide.
- Local artists, creators, and cultural producers can use online platforms to gain visibility and access global markets, transcending geographical boundaries and cultural barriers.
- Conversely, the dominance of global platforms can also lead to the homogenization of culture, as content that conforms to dominant cultural norms and tastes tends to receive greater visibility and popularity.

2. Algorithms:

- Algorithms influence the visibility and dissemination of cultural content on online platforms. They may prioritize popular or trending content, amplifying the reach of global cultural products while marginalizing local or niche content.
- This can lead to a "winner-takes-all" dynamic, where a few blockbusters cultural products dominate the online landscape, crowding out diverse and locally-produced content.
- However, algorithms can also facilitate the discovery of niche or independent cultural content by recommending personalized recommendations based on users' interests and behaviors.