

6

Impacts of Computing



Learning Outcomes

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

- understand and apply safe & responsible use of the internet to prevent addiction, promote information and data security
- evaluate the impact of and apply strategies to prevent cyberbullying/harassment
- analyze the impacts of the digital divide on access to critical information



UNIT INTRODUCTION

Using the internet safely is very important today. This unit will help you learn how to be careful and responsible online. We will discuss here how to avoid internet addiction and keep your personal information safe. It is also important to protect your personal information. Using strong passwords, looking out for scams, and keeping your privacy settings updated can help protect you from online threats and keep your digital identity safe.

Spending too much time online can harm your mental health and lesser your productivity. By noticing when you are spending too much time online and finding ways to reduce it, you can keep a healthy balance in life.

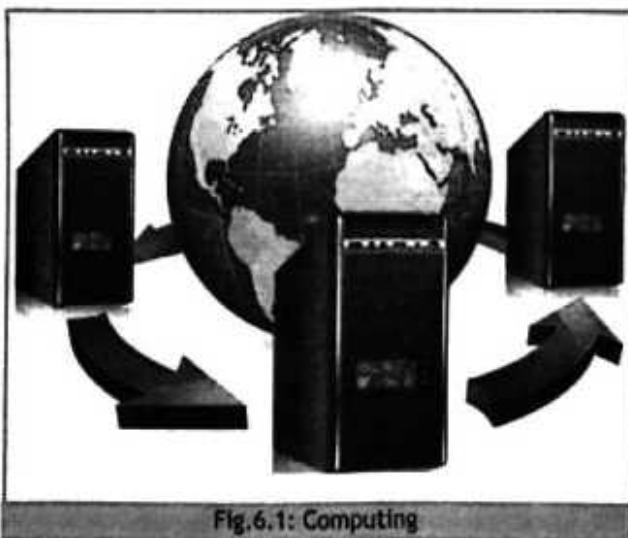


Fig.6.1: Computing

6.1 What is Technology Addiction

Technology addiction, also known as digital or internet addiction, refers to the excessive and compulsive use of devices like smartphones, computers, video games, and social media. This type of addiction can disrupt a person's daily life, relationships, and overall well-being, similar to other behavioral addictions like gambling or compulsive shopping.

Activities that often lead to technology addiction include heavy use of social media, online gaming, video streaming, endless web browsing, and constant texting or messaging. However, not everyone who uses technology a lot is addicted. The key difference is whether the technology use negatively affects one's life and if the person struggles to control it. Technology addiction is a serious issue that might require treatment through counseling, therapy, support groups, and strategies to use technology more responsibly.



Fig.6.2: Technology addiction

Teacher Point:

In a remote village, Sara struggles to access online educational resources due to limited internet availability, while her friend in the city excels with high-speed connectivity. The teacher helps students analyze how the digital divide creates unequal opportunities, affecting access to critical information for education, healthcare, and job opportunities, emphasizing the need for equitable solutions.

6.1.1 Concern of technology addiction

Technology addiction is a rising question in today's world. It affecting people of all ages. Spending too much time on devices, social media, and games can make people excessively dependent on technology, which can harm both their mind and body. It is important to understand this problem and find ways to control technology use to keep a healthy balance between online activities and real-life relations.

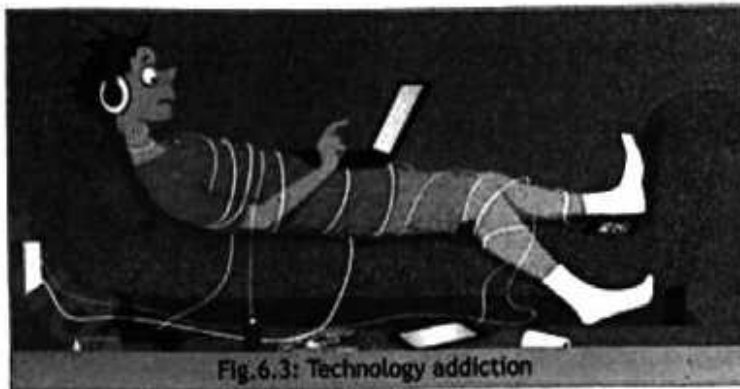


Fig.6.3: Technology addiction

Mental Health Challenges:

Depression and Anxiety:

Technology addiction can make feelings of depression and anxiety worse because always comparing yourself on social media, dealing with cyberbullying, and facing online harassment can hurt your mental health.

Isolation:

Excessive screen time can cause social isolation and loneliness. When people spend too much time on screens, they have less face-to-face interaction. Technology addiction can also harm relationships with family and friends. This happens because people may choose their devices over real conversations.



Fig.6.4: Mental Health Challenges

Academic and Occupational Problems:

Decreased Productivity:

Technology addiction can lead to decreased productivity at work or in school due to constant distractions.

Academic Underperformance:

Students addicted to technology may find it hard to focus on their studies, which can affect their grades and academic performance.



Fig.6.5: Academic and Occupational Problems

Privacy and Security Concerns:

Oversharing:

People who are addicted to social media might share too much personal information, which can put their privacy and security at risk.

Online Scams and Cybersecurity Risks:

People who are addicted to technology might be at higher risk of falling for online scams and cyberattacks because they spend too much time online.



Fig.6.6: Privacy and Security Concerns

Analyze the impact of new technology laws on digital privacy:

New technology laws have changed digital privacy and security in both good and bad ways. These laws, such as GDPR in Europe and CCPA in the U.S., help people control their personal information and require companies to protect data more carefully. They also help by making companies report data leaks quickly. However, finding a balance between privacy and letting law enforcement access data is tough and can impact people's privacy. For businesses, following these rules can be expensive, and different laws in each country make it harder to manage data internationally.

6.2 Internet

The internet is like a giant web connecting computers and devices everywhere. It allows us to share information, communicate, online buying and selling, and watch videos etc. Think of it as a massive library where you can find almost anything you want to learn. The internet has revolutionized how we live and work, continuously improving with new advancements. It is now a crucial part of our daily lives, making tasks quicker and simpler than ever before.



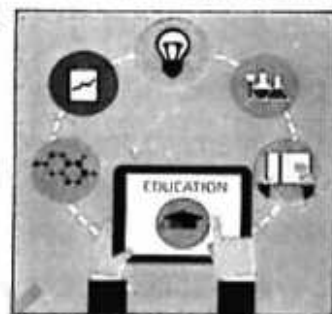
Fig.6.7: Internet

6.2.1 Use internet for beneficial purposes

Using the internet for good purposes like to help people and communities. This includes using online tools for learning, health, social interaction, and caring for the environment. The internet connects people, making it easy to share ideas and work together. This introduction explores how the internet can bring positive changes, inspire people, and improve lives.

Information and Education:

The internet provides access to a vast amount of information and educational resources. It has made learning more accessible through online courses, tutorials, and educational websites, enabling people to acquire new skills and knowledge.





Global Communication:

The internet links people from all over the world, making it simpler for individuals to talk with family and friends who are far away. It has also helped people work together internationally and share different cultures.

Social Activism:

Social media sites and online groups have played a big role in making people more aware of social and environmental problems. Activities like climate change activism have become more popular and have made a difference because of online efforts.

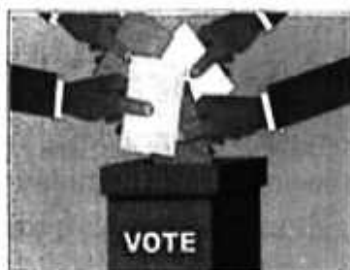


Medical Information and Telemedicine:

Getting medical information and using telemedicine services online has made it easier for people to get healthcare, especially in areas where there are not many doctors or hospitals nearby. Patients can talk to healthcare professionals and find medical help online.

Support Communities:

Communities and support groups online are available for individuals facing different difficulties like mental health problems, addiction, or long-term illnesses. These groups give people a feeling of belonging and provide resources for those needing support and guidance.



Political Engagement:

The internet has boosted citizen involvement in politics by giving them places to chat about political topics, sign up for voting, and join in elections. Plus, it is made government actions more visible and open.

Cultural Exchange:

The internet allows people from different cultures to connect and share their traditions, art, and ideas. It promotes cultural understanding and appreciation.



Innovation and Research:

Scientists and researchers can collaborate and share their findings online, accelerating the pace of innovation and discovery across various fields.



6.2.2 Use of internet for malicious purposes

The internet is a potent tool that has both good and bad effects on society. While it makes it easier to access information and communicate, it also allows for cybercrime, online harassment, and the spread of illegal content. From cyberterrorism to scams and privacy breaches, the internet poses a range of challenges. While steps are taken to fight online crime, users also need to stay alert and practice online safety to reduce risks.



Cybercrime:

Criminals use the internet for various illegal activities, including hacking, identity theft, online fraud, and spreading malware. These actions can lead to financial losses, data breaches, and damage to individuals and organizations.

Online Harassment



Online Harassment and Bullying:

The secrecy provided by the internet can encourage some individuals to engage in cyberbullying, harassment, and trolling, causing emotional distress and harm to others.



Cyberterrorism:

Cyberterrorism is when the internet is used to attack computer systems or networks for political or ideological reasons, intending to create fear, chaos, or harm. This can involve actions like hacking into government websites, causing problems with essential services, or spreading propaganda online. The aim is to cause fear or push forward a specific agenda by using technology.

Illegal Content:

The internet is used to distribute and share illegal content, such as child abuse, pirated software, and copyrighted materials without permission.



Hate Speech and Disinformation:

Some individuals and groups use the internet to spread hate speech, misinformation, and disinformation, which can contribute to social division and tension.



Online Scams:

Scammers often use the internet to trick individuals into giving away personal information or money through various fraudulent schemes, including phishing (Phishing is a scam that tricks people into giving away personal information, like passwords, by pretending to be someone trustworthy) emails and fake websites (Fake websites are imitation sites designed to look real but are created to steal personal information or spread malware).

Privacy Violations:

There are instances where the internet is exploited to invade people's privacy, such as by hacking into personal devices or leaking sensitive information.



Cyber Espionage:

Nation-states and other entities may engage in cyber espionage to steal sensitive information, intellectual property, and government secrets.

6.3 The Effects of Threats to Individual Privacy and Security

Threats to individual privacy and the security of data from spam, spyware, and cookies are significant concerns in the digital age. Each of these threats has distinct implications and can pose various risks to users:

Spam:

Spam emails usually have annoying ads or harmful stuff. If you get spam, If you receive spam, it could mean someone got your email without your permission, which can put your privacy at risk. Some spam emails even have viruses or try to trick you into giving personal info by clicking immoral links or downloading corrupt files. To deal with spam, you can use spam filters, be careful who

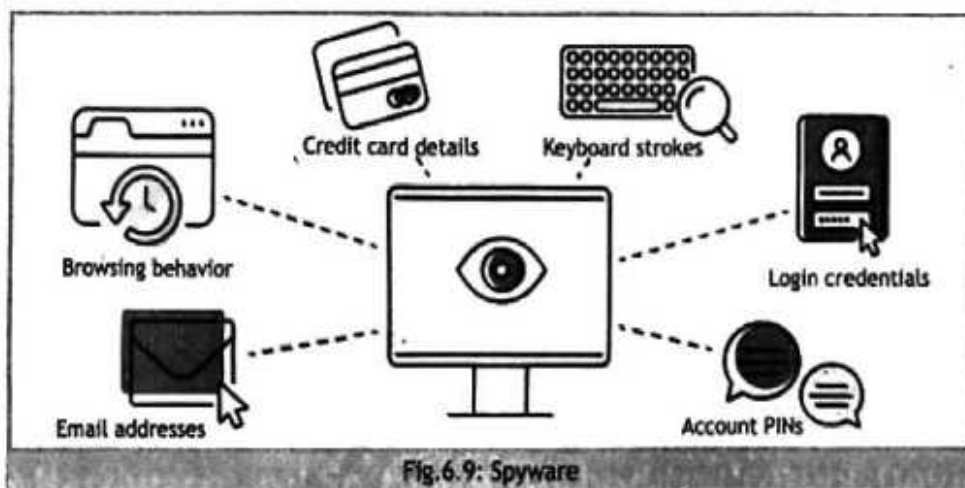


Fig.6.8: Spam emails

you share your email with, and tell your email provider about spam. Using temporary email addresses for online stuff can also help avoid spam.

Spyware:

Spyware is software that spies on what you do on your device, takes your personal info, and sends it to unauthorized people. This invasion of privacy can lead to someone stealing your identity or money. Spyware can also make your device unsafe by letting people access important information. It can see what you type, take pictures of your screen, and remember your passwords. To stay safe from spyware, always update your antivirus and anti-spyware software. Do not download software from places you do not trust, and be careful with links and files you click on.

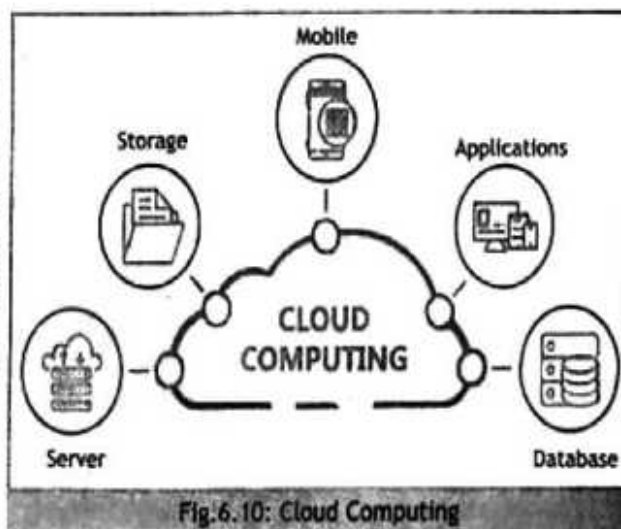


Cookies:

Cookies are tiny files saved on your device to remember what you do online. Some cookies are okay, but others collect your information without asking, which is not good for your privacy. You can control and remove cookies in your web browser settings. Also, turning on settings to block cookies from other websites can help keep privacy safe.

6.4 Cloud Computing

Cloud computing is a way to use computer stuff like servers, storage, and software over the internet. Instead of having to buy and manage all the hardware yourself, you can rent it from companies that offer cloud services. This setup has many advantages, like being able to change how much you use based on your needs, saving money, being flexible, and accessing your stuff from anywhere with internet.



6.4.1 Public cloud

A public cloud is a type of cloud computing service that provides resources and services over the internet to multiple users and organizations. It is called "public" because the cloud infrastructure is owned and operated by a third-party cloud service provider and is made available to the general public or a wide range of customers. These cloud providers typically have vast data centers with a multitude of servers, storage, and networking equipment that they use to deliver various cloud services.



6.4.2 Private cloud

A private cloud is a cloud computing environment that is exclusively used by a single organization or entity, such as a business or government agency. Unlike public clouds, which are shared by multiple users and hosted by third-party providers like Amazon Web Services (AWS) a private cloud is typically hosted and managed within the organization's own data centers.

6.4.3 Basics of security and privacy of cloud computing

Security and privacy are critical aspects of cloud computing. When using cloud services, whether for personal or business purposes, it is essential to understand the basics of how security and privacy are managed. Here are the key concepts and considerations:

Data Encryption:

Make sure that data sent to and from the cloud is encrypted using secure methods. Data stored in the cloud should also be encrypted to keep it safe from unauthorized access. Cloud providers usually offer encryption options for data that is stored.



Access Control:

Create strong access control rules to limit who can use resources in the cloud. Use tools like Identity and Access Management (IAM) to manage user permissions. Use strong authentication methods, like multi-factor authentication (MFA), to improve security when accessing accounts.

Incident Response and Monitoring:

Set up tools to watch for any strange or suspicious actions in your cloud system. Create a plan to quickly handle any security problems if they happen.

Privacy Policies and Data Handling:

Review the privacy policies of cloud provider to understand how they handle data. Minimize the amount of personal or sensitive data stored in the cloud and only store what is necessary.

Network Security:

Use firewall rules, network segmentation, and Virtual Private Cloud (VPC) to secure your cloud resources. Keep an eye on network traffic and use tools to detect and respond to any suspicious activity.

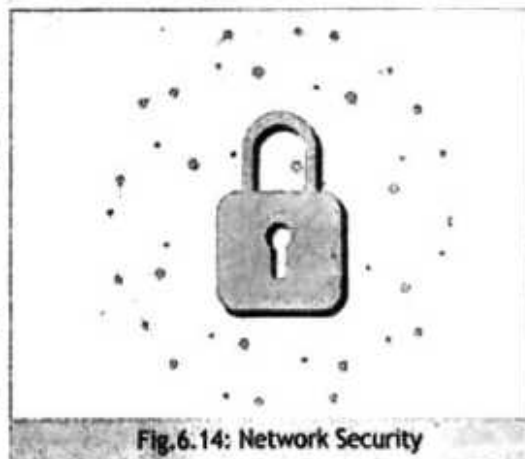


Fig. 6.14: Network Security

6.5 Hardware and Software Method to Protect Devices

Using both hardware and software is really important to keep devices safe from different kinds of dangers. Hardware methods include things like using your fingerprint to unlock your device, or special technology to keep your information safe. It also means using special walls for your internet to stop bad things from getting in. Software methods are different; they involve installing programs on your device to stop viruses and other bad stuff. It also means updating your programs often to fix any problems and adding extra steps to make sure it is really you logging in. By using both hardware and software approaches, devices can stay safe from online dangers and people trying to get in without permission.

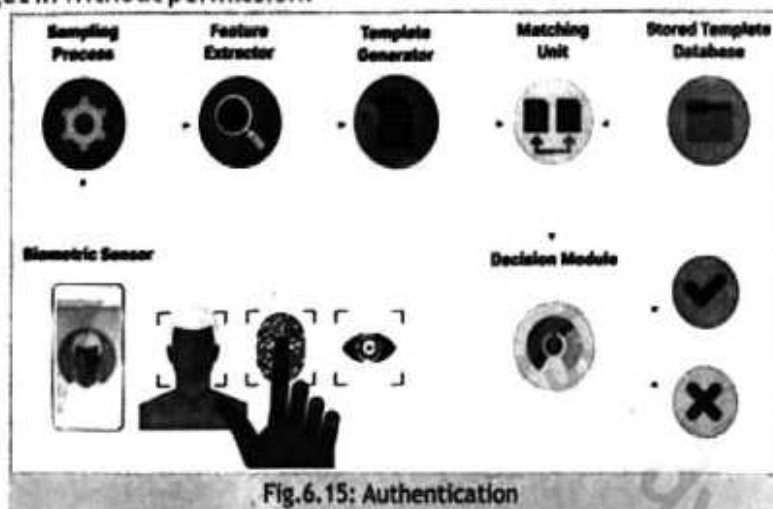


Fig. 6.15: Authentication

6.5.1 Hardware Methods

Biometric Authentication:

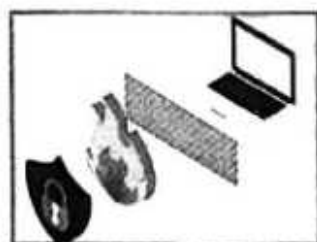
Many modern devices come equipped with biometric sensors, such as fingerprint scanners or facial recognition cameras. These hardware components provide an extra layer of security by ensuring that only authorized users can access the device.



Secure Boot:

Secure boot is a hardware-based process that ensures only trusted software is loaded during the device startup. It prevents malware from infecting the boot process.

Firewalls:



A firewall is a security system that helps protect computers and networks from unauthorized access. It acts like a barrier, blocking unwanted traffic from entering or leaving a network while allowing safe, approved traffic to pass through. Firewalls help keep personal and sensitive information secure by filtering out potential threats, such as hackers or malware, before they can reach your device or network.

6.5.2 Software Methods

Antivirus and Antimalware Software:

Install reputable antivirus and antimalware software to regularly scan and protect the device from known threats. Keep these programs up to date to defend against new threats.



Operating System Updates:

Regularly update the operating system and software applications. Updates often include security areas that address weaknesses that hackers can exploit.

Firewalls (Software):

Use a software firewall, in addition to any hardware firewall, to control the traffic to and from the device. Configure it to block unauthorized access and outgoing data leaks.

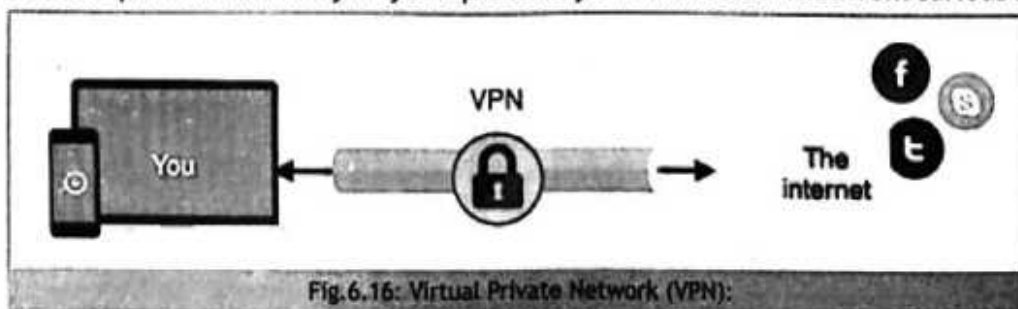
Password Management:

Use strong, unique passwords for each account and employ a password manager to store and manage them securely. Two-factor authentication (2FA) should also be enabled wherever possible.



Virtual Private Network (VPN):

A VPN encrypts your internet connection, making it more difficult for cybercriminals to intercept your data. It also helps maintain anonymity and protects your online activities from curious eyes.



Data Backup:

Regularly back up your important data to an external device or cloud storage service. In the event of data loss due to malware or hardware failure, you can restore your information.

6.6 Cybersecurity

Cybersecurity refers to the practice of protecting computer systems, networks, and data from unauthorized access, cyberattacks, and other malicious activities. It involves implementing a range of technologies, processes, and practices to safeguard digital assets and ensure the confidentiality, integrity, and availability of information. Cybersecurity measures aim to defend against various threats, including malware, phishing scams, ransomware, and insider threats, among others. By implementing robust cybersecurity measures, individuals, organizations, and governments can mitigate risks, prevent data breaches, and preserve trust in the digital ecosystem.



Fig.6.17: Cybersecurity



Fig.6.18: Need of cybersecurity

6.6.1 Need of cybersecurity

Cybersecurity is crucial for protecting privacy and information security in our digital era. As technology advances and systems become more interconnected, the amount of data exchanged online grows rapidly, posing significant challenges for privacy and security. Without strong cybersecurity measures, personal data like financial records and medical histories are at risk.

It is being accessed or exploited by malicious actors;

leading to identity theft and other serious consequences. Additionally, cybersecurity is closely linked to data security, which involves safeguarding information from unauthorized access or alteration. In conclusion, by prioritizing cybersecurity measures, we can protect sensitive data and maintain trust in our digital world.

6.6.2 Cybercrimes laws

Cybercrime laws are rules made to stop illegal activities using computers or digital tools. They explain what cybercrimes are and set punishments for those who commit them. They also guide police on how to catch and punish cybercriminals. Cybercrimes include hacking, identity theft, fraud, data breaches, cyberbullying, online harassment, stealing intellectual property, and cyber terrorism. Examples are breaking into computer systems, phishing scams, malware attacks on websites.



Fig.6.19: Cybercrimes laws.

6.6.3 Instances of Cybercrimes

Cybercrimes involve various illegal activities done online. Examples include stealing personal information like social security or bank details to impersonate someone. Tricking people through emails or fake websites to get sensitive data is another example. Deploying harmful software like viruses to steal data or disrupt systems is also a cybercrime. Hacking into networks to steal important information is common. Running scams online to deceive and extort money is another form of cybercrime. Harassing or threatening others through social media is also included. Flooding websites with traffic to make them unusable is a type of attack. Stealing information or government secrets through espionage is another example. Misusing access to systems or data is also a cybercrime. Exploiting minors through online platforms is a serious cybercrime. These examples show the different types of cybercrimes that exist today.

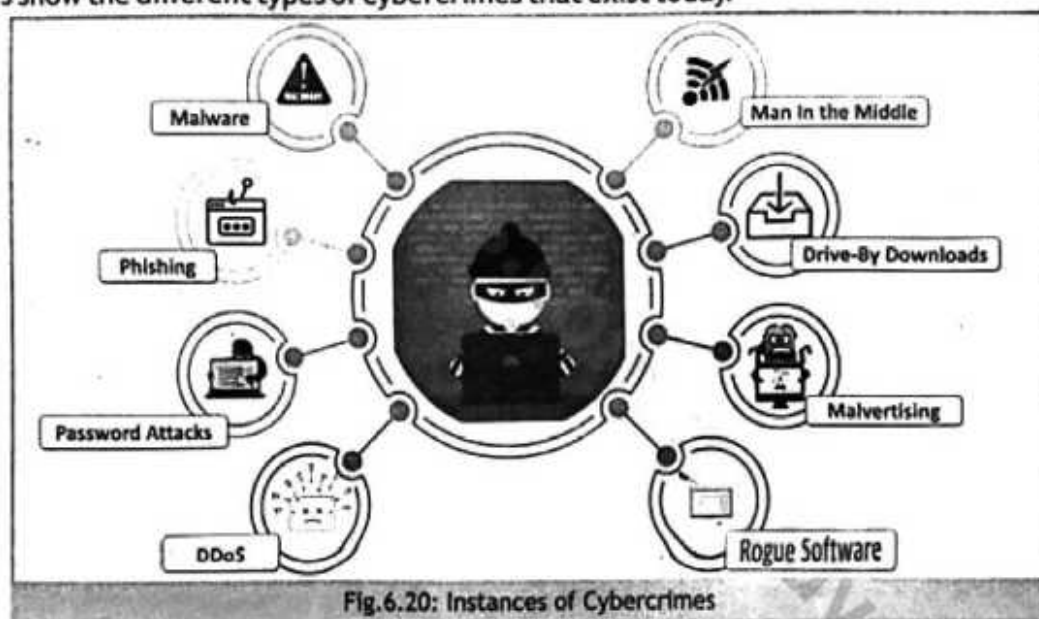


Fig.6.20: Instances of Cybercrimes

6.6.4 Common methods of reporting cybercrimes

Law Enforcement Agencies:

Reporting Cybercrime Contacting local police departments or national law enforcement agencies to report cybercrimes. Many countries have specialized cybercrime units or task forces dedicated to investigating and prosecuting cybercrimes.

Government Agencies:

Reporting cybercrimes to government agencies responsible for cybersecurity and digital crimes. These agencies often have dedicated hotlines, online reporting portals, or email addresses where individuals can report incidents and seek assistance.

Internet Service Providers (ISPs):

Informing ISPs about cybercrimes, especially if the incidents involve illegal activities conducted through their networks or services. ISPs may take action against malicious users or provide assistance in reporting incidents to relevant authorities.

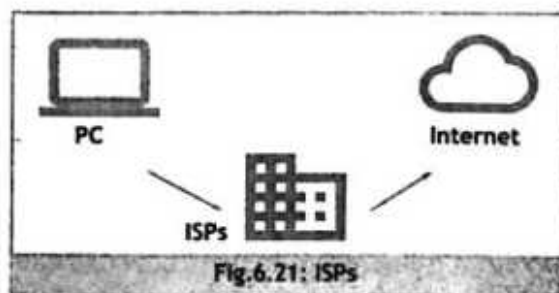


Fig.6.21: ISPs

Financial Institutions:

Notifying banks or financial institutions if cybercrimes involve unauthorized access to accounts, fraudulent transactions, or other financial crimes. Financial institutions often have procedures in place to investigate and address such incidents.

Online Reporting Portals:

Report cybercrimes using online portals set up by government agencies, law enforcement, or cybersecurity organizations. These platforms allow to report crimes anonymously or ask for help with cyber threats. By using these reporting methods, people and organizations help detect, investigate, and prosecute cybercrimes. This effort helps fight cyber threats and improve cybersecurity.



Fig.6.22: Online Reporting Portals

6.7 Safety and Security Concept

Safety and security on social media involve many challenges, such as protecting privacy, dealing with online harassment, cyberbullying, and peer pressure. To solve these problems, everyone needs to work together, including platform operators, policymakers, teachers, parents, and users. Promoting digital literacy and building supportive communities can make a difference. It is also important to put strong safety measures in place. By working together, we can create a safer and more positive online space for everyone.

Privacy Protection:

Social media platforms collect a lot of personal data, which raises privacy concerns. Users can protect their privacy by adjusting privacy settings. They should be cautious about sharing sensitive information. Regularly reviewing online profiles for publicly visible content is also important.

Online Harassment and Cyberbullying:

Online Harassment/Cyberbullying is when people use the internet to bully or scare others. This can really hurt the feelings and mental health of the victims. To stop cyberbullying, we can teach everyone how to behave nicely online. It's important to encourage kindness and respect. We should also have easy ways for people to report bullying and get help.

Peer Pressure and Social Influence:

Peer pressure and social influence can make people feel like they need to act a certain way to be accepted by others. This can lead to taking risks or making unhealthy choices. To stay safe and secure, it is important to learn how to make good decisions on your own. Building self-confidence helps you resist pressure. Creating supportive groups where everyone feels valued can also reduce the negative effects of peer pressure.

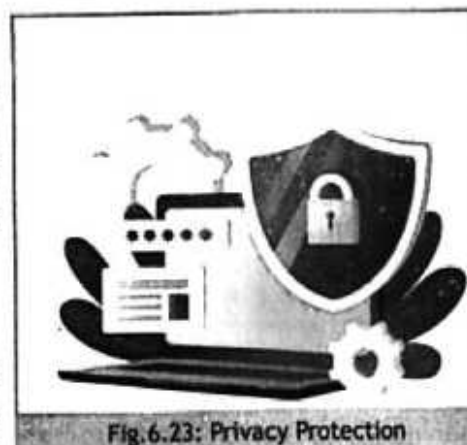


Fig.6.23: Privacy Protection

6.8 Cyberbullying

Cyberbullying is when someone uses the internet or digital devices to hurt, harass, or intimidate others. This can include mean messages, spreading rumors, or sharing private information to embarrass someone. It can happen on social media, through text messages, or in online games. Cyberbullying can make the victim feel very upset and unsafe.



Fig.6.24: Cyberbullying

6.8.1 Impact of Cyberbullying/Harassment

Psychological Effects:

Victims often experience anxiety, depression, low self-esteem, and even suicidal thoughts. The constant fear and humiliation can have long-lasting psychological consequences.

Academic and Professional Impact:

Cyberbullying can make it hard for someone to focus on school or work, causing their performance to drop. It can also damage their professional reputation and future job opportunities.

Social Isolation:

Victims may stop joining social activities and feel alone. They might lose trust in others and find it hard to make new friends or relationships.

Physical Health:

The stress from online harassment can lead to physical health problems, such as headaches, sleep disturbances, and stomach issues.

Consequences of Cyberbullying:

Cyberbullying and harassment can have serious effects on a person. It can lead to stress, anxiety, and depression. Victims might struggle to focus on school or work, and their performance may suffer. They may feel alone, lose confidence, and have trouble trusting others or making new friends. In some cases, it can even harm their reputation and future job opportunities. Overall, it can deeply hurt both their mental health and social life.



Fig. 6.25: Impact of Cyberbullying/Harassment

6.8.2 Strategies to Prevent Cyberbullying/Harassment

Education and Awareness:

Promote digital literacy and raise awareness about the consequences of cyberbullying among both children and adults. Teach responsible online behavior and empathy.

Parental Involvement:

Parents should be actively involved in their children's online activities. Setting rules and monitoring their internet usage.

School and Workplace Policies:

Schools and workplaces should have clear anti-cyberbullying policies in place. These policies should outline consequences for criminals and provide support for victims.

Reporting Mechanisms:

Establish anonymous reporting systems for victims and witnesses to report cyberbullying incidents. Ensure that reports are taken seriously and acted upon promptly.



Social Media Regulation:

Encourage social media platforms to implement stricter policies against cyberbullying and harassment. Platforms should swiftly remove harmful content and ban repeat lawbreakers.

6.9 The Environmental, Cultural and Human Impact of Computing and Assistive Technologies

Computing and assistive technologies affect the environment, culture, and people in many ways. They can improve lives by making tasks easier, especially for those with disabilities. However, producing and using these technologies can impact the environment due to energy use and electronic waste. They also influence cultures by changing how we communicate, learn, and work.

6.9.1 Environmental Impact

The environmental impact of computing and assistive technologies includes high energy use and electronic waste. Devices like computers and data centers need a lot of electricity, which can lead to pollution and greenhouse gas emissions. As technology advances, devices are often quickly replaced, creating electronic waste (e-waste) with harmful materials that can harm the environment if not safely recycled. Efforts are being made to reduce these impacts, but challenges remain.



Fig.6.26: Energy Consumption

6.9.2 Cultural Impact

The cultural impact of computing and assistive technologies is seen in how they change the way people interact, learn, and work. These technologies make it easier to connect across distances, share information, and access educational resources. They also help people with disabilities participate more fully in society. However, they can also lead to less face-to-face communication and may create a digital divide. This gap can make cultural and economic differences.

6.9.3 Human Impact

The human impact of computing and assistive technologies is both positive and challenging. These technologies make tasks easier, especially for people with disabilities, helping them to communicate, learn, and work better. However, using technology too much can cause problems like addiction, stress, and less physical activity. Also, technology is always changing, which can lead to job changes and challenges in learning new tools.



Fig.6.27: Human Impact

6.10 Digital Divide

The digital divide means some people or groups have less access to technology, like the internet, compared to others. This gap can show up in different ways and affect individuals, groups, or even whole areas. It is a big deal because it can cause problems in society, the economy, and politics.



Fig.6.28: Digital Divide

Analyze the impacts of the digital divide on access to critical information:

The digital divide limits access to critical information, especially for those without reliable internet, devices, or digital skills. People in low-income, rural, or underserved areas often miss out on essential services like online education, healthcare, and job opportunities. This divide worsens social inequalities, leaving some groups without important resources or timely information. Bridging the digital divide can improve equity, giving everyone a fair chance to connect, learn, and grow.

6.10.1 Access Divide

Infrastructure:

One aspect of the digital divide is access to the physical infrastructure. The infrastructure required for digital connectivity, including broadband internet, computers, and mobile devices. Rural or remote areas often have limited or no access to high-speed internet, creating an urban-rural divide.

Affordability:

Even when infrastructure is available, cost can be a barrier. Internet service, computers, and smartphones can be expensive for low-income individuals and families, making them inaccessible.

6.10.2 Usage Divide

Digital Literacy:

Just having access to technology is not enough. People also need to know how to use it well. Some, especially older people, might not have the skills to use digital tools and the internet properly.



Relevance of Content:

Some people can use the internet, but they might not see it as important for their everyday life. This could be because there is not much content available in their language or about things that matter to them.

6.11 Inequitable Access to Information

When some people do not have the same access to information or technologies as others, it can really affect their lives. Imagine if you could not find out important things or learn new stuff because you did not have the same access to books or the internet as other people. It might make it harder to do well in school or find a good job. Having fair access to information is really important for everyone to have the same opportunities.



Fig. 6.29: Inequitable Access to information

Case Study

Apply Safe & Responsible Use of the Internet

Scenario:

Ali, a Grade 10 student, loves using the internet for studying, gaming, and socializing with friends. However, he recently noticed that he spends too much time online, which affects his studies and sleep. Additionally, he sometimes receives strange friend requests and messages from unknown people on social media, which makes him feel uncomfortable. He is also unsure if the websites he visits are safe and if his personal information is secure.

Ali's school has introduced a session on responsible internet use, focusing on the importance of balancing online activities, recognizing safe websites, and protecting personal information.

Objective:

To help Ali and his classmates "apply safe & responsible use of the internet to prevent addiction, promote information and data security." Demonstrates how students can apply safe and responsible internet practices to balance their online activities, avoid addiction, and ensure information and data security.

Unit Summary

- **Internet Safety:** The practice of using the internet in a secure and responsible manner to protect personal information and avoid online threats.
- **Internet Addiction:** Compulsive and excessive use of the internet that interferes with daily life, relationships, and well-being.
- **Cyberbullying:** Online harassment or bullying that can cause emotional distress and has significant negative impacts on individuals.
- **Technology Addiction:** Compulsive and excessive use of digital devices and platforms, leading to negative effects on mental health, productivity, and relationships.
- **Internet:** A global network of interconnected computers and devices that allows for the sharing of information and communication.
- **Spam:** Unwanted and often malicious emails that compromise user privacy and security.
- **Spyware:** Malicious software that secretly monitors and collects personal information from users.
- **Cookies:** Small text files stored on a user's device to track online activity, which can raise privacy concerns.
- **Cloud Computing:** Technology that provides access to computing resources and services over the internet, allowing for scalable and flexible use of IT infrastructure.
- **Public Cloud:** Cloud computing services offered over the internet by third-party providers to multiple users.
- **Private Cloud:** A cloud computing environment exclusively used by a single organization, offering more control over data and security.
- **Data Encryption:** The process of converting data into a coded format to prevent unauthorized access.
- **Access Control:** Policies and mechanisms that restrict access to resources based on user roles and permissions.
- **Network Security:** Measures taken to protect data during transmission over networks, including firewalls and intrusion detection systems.
- **Biometric Authentication:** Security measures that use biological characteristics, such as fingerprints or facial recognition, to verify identity.
- **Secure Boot:** A hardware-based process ensuring only trusted software is loaded during startup, protecting against malware.
- **Antivirus Software:** Programs designed to detect, prevent, and remove malware from devices.

- **VPN (Virtual Private Network):** A service that encrypts internet connections, enhancing privacy and security.
- **Data Backup:** The practice of regularly saving copies of important data to prevent loss due to cyber threats or hardware failures.
- **Cybersecurity:** The practice of protecting computer systems, networks, and data from unauthorized access, cyberattacks, and other malicious activities.
- **Cybercrime Laws:** Rules designed to prevent illegal activities using computers or digital tools, defining cybercrimes and setting punishments for offenders.
- **Digital Divide:** The gap between individuals or communities with access to digital technologies and those without, affecting societal, economic, and political opportunities.
- **Access Divide:** The disparity in access to physical infrastructure and affordability of digital technologies between urban and rural areas and among different income groups.
- **Usage Divide:** The gap in digital literacy and relevance of content, impacting individuals' ability to effectively use technology.
- **Participation Divide:** The disparity in engagement in online activities, economic opportunities, and access to online services due to lack of technology or skills.
- **Global Divide:** The worldwide disparity in access to technology and digital resources between richer and poorer countries.

Exercise

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

1. _____ is a key reason for being careful and responsible online?
 - a) To save money
 - b) To avoid technology addiction and protect personal information
 - c) To become more popular
 - d) To learn new skills
2. Spending too much time online be harmful for?
 - a) Mental health and productivity
 - b) Physical fitness and diet
 - c) Shopping habits
 - d) Travel plans
3. Which of the following is NOT a way to protect personal information online?
 - a) Using strong passwords
 - b) Being alert for scams
 - c) Sharing your passwords with friends
 - d) Keeping privacy settings updated
4. Technology addiction is well described by
 - a) Using technology occasionally
 - b) Excessive use of digital devices
 - c) Avoiding all forms of technology
 - d) Only using technology for work purposes
5. What is a common result of excessive screen time?
 - a) Enhanced social skills
 - b) Social isolation and loneliness
 - c) Improved academic performance
 - d) Increased physical activity
6. Which of the following is a way to reduce technology addiction?
 - a) Increasing online gaming hours
 - b) Practicing mindful use of technology
 - c) Ignoring signs of addiction
 - d) Sharing personal information online
7. Select one benefit of using the internet for good purposes?
 - a) Increasing online fraud
 - b) Access to educational resources
 - c) Spreading misinformation
 - d) Cyberbullying
8. _____ of the following is a positive use of the internet?
 - a) Cybercrime
 - b) Online harassment
 - c) Supporting social meeting
 - d) Distributing illegal content
9. _____ is a way to protect your device from online threats?
 - a) Avoid using antivirus software
 - b) Ignore software updates
 - c) Use biometric authentication
 - d) Share passwords freely

-
10. Which method is a hardware method to protect devices?
- a) Biometric authentication
 - b) Secure boot
 - c) Firewalls
 - d) All
11. What is a public cloud?
- a) A cloud environment used by one organization
 - b) A cloud service offered to the general public by a third-party provider
 - c) A private network for personal use
 - d) A secure boot process for devices
12. ____ is the primary goal of cybersecurity?
- a) To increase internet speed
 - b) To protect computer systems and networks
 - c) To develop new software applications
 - d) To create more social media platforms
13. Which of the following is an example of a legal online activity?
- a) Hacking into a network to steal information
 - b) Tricking people through phishing scams
 - c) Developing a new mobile app
 - d) Deploying malware to disrupt systems
14. Why is cybersecurity essential in the digital era?
- a) It helps in faster data transmission
 - b) It reduces the need for technical support
 - c) It decreases the cost of internet services
 - d) It ensures that personal data is protected, from malicious actors
15. Role of students which can minimizing the digital divide?
- a) Developing new gaming applications
 - b) Providing technology training and support to those who need it
 - c) Reducing the prices of digital devices
 - d) Creating more social media accounts

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

1. List the importance of safely use of internet today?
2. State four ways to protect personal information online?
3. Mention three benefits of cloud computing?
4. Why is cybersecurity essential in today's digital era?
5. Name three common types of cybercrimes.
6. What would you do if your friend faced cyberbullying?

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

1. What are the impacts of cyberbullying and online harassment, and what strategies can be implemented to prevent them?
2. Describe the various threats that cybersecurity measures aim to defend against.
3. Explain the role of cybercrime laws in addressing illegal activities conducted through digital tools.
4. Analyze the cultural impact of computing technologies. How do these technologies facilitate global connectivity and cultural exchange.
5. Examine the effects of the digital divide on access to information. How does this divide affect education, employment, healthcare?



Activity-1

Safe and Responsible Use of the Internet

Grade 10 students will learn about safe internet use to prevent addiction and enhance data security. Over two class periods, students will discuss internet safety, research related topics, and present their findings. They will create posters promoting responsible internet use and participate in a gallery walk to view and comment on their peers' work. Assessment includes participation, presentations, and creative posters. A reflection homework assignment will reinforce the principles learned.



Activity-2

Preventing Cyberbullying and Harassment

Grade 10 students will evaluate the impact of cyberbullying and learn strategies to prevent it. In groups, they will research the effects of cyberbullying and present their findings. Each group will create an anti-cyberbullying campaign poster. The class will discuss effective prevention strategies and display their posters around the school to raise awareness.

Teacher Points:

"Evaluate the impact of and apply strategies to prevent cyberbullying/harassment"

1. Understanding Cyberbullying

- Define cyberbullying and explain how it can occur on various online platforms (social media, messaging apps, games, etc.).
- Discuss the forms it can take, such as harassment, spreading rumors, impersonation, and exclusion.

2. Evaluating the Impact

- Explain the effects of cyberbullying on victims, including emotional stress, anxiety, depression, and academic struggles.
- Share real-life examples or case studies to illustrate the seriousness of these impacts.

3. Recognizing Signs of Cyberbullying

- Teach students how to recognize if they or others are being cyberbullied (e.g., feeling scared to check messages, changes in mood or behavior).

4. Strategies to Prevent Cyberbullying

- Encourage respectful communication and responsible online behavior.
- Teach students how to adjust privacy settings, block/report users, and avoid engaging with negative comments.
- Discuss the importance of supporting peers who may be victims of cyberbullying.