



Cyber Safety



Learning Outcomes

- Internet
- Advantages and Disadvantages of the Internet
- Computing Ethics
- Unethical Practices
- Cyber Crime
- Safety Measures while using
- Computer and Internet

Internet

The internet is one of the largest information databases. It has become a vital part of our lives. Internet stands for **Interconnected Network** of computers. It is a global system of inter-connected computer networks that enables the user to share information and various resources with each other. It uses common communication standards and interfaces to provide the physical backbone for many interesting applications.

Tasks that were usually performed through personal interaction, such as banking, shopping or communication, can now be done online. We can share data and information across the globe instantly. Indeed, the internet has transformed the world into smaller and convenient place to live in. The scope of internet is getting wider with each passing day.

1

To analyse how fast the internet is growing, pick any newspaper or magazine, and carefully observe the advertisements given therein. You would realize that almost every enterprise has its website listed in addition to its address and

telephone numbers. Every organization is making its presence felt on the internet. The internet is a boon to the world as the 24x7 operation of the internet has revolutionized almost every aspect of our life.



Advantages of the Internet

Education : The internet has changed the traditional learning system. It is widely used for educational purpose by scholars, students, and teachers to learn anytime and anywhere.



It has shown dramatic impact on higher education as a growing number of universities offer online courses. IGNOU is one such university which offers this facility. The internet is a vast storehouse of information and is also used to publish papers and articles.

Convenient mode of Communication : The internet provides a convenient and economical mode of communication. Users can communicate with each other using various services available on the internet like e-mail, chat, video conferencing, instant messenger, etc.

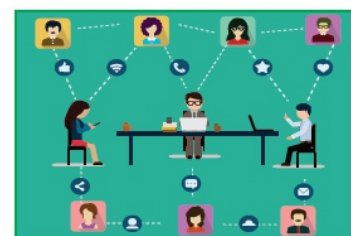


Business : The internet has brought new opportunities for businesses to sell goods and services online, which has proven to be beneficial. Meeting can be conducted economically through the video conferencing facility, without physically visiting the place. Financial transactions can be made online from office or home.

E-Commerce : It is the concept used for any type of commercial or business deal that involves the transfer of money across the globe by using the internet. Nowadays, many companies have their own portals/websites, which are used for E-commerce. E-commerce industry has become one of the biggest industries in the world. We can now purchase a variety of good and get services from different shopping portals around the world. It also includes booking hotel rooms, and tickets for bus, flight, and train.



Media and Entertainment : The internet has facilitated the media and entertainment industry. Downloading games, videos, songs, visiting chat rooms, or surfing the web, are some of the uses which attract people towards the internet. The internet also provides the facility to read different newspaper, magazines, and books online.



Social Networking : It is the latest way to communicate. It offers a platform where an individual can connect with friends and strangers on the basis of shared interests or views. Some examples of social networking sites are: Facebook, Twitter, LinkedIn, MySpace, etc.

Forum : An internet forum is online discussion site where like-minded people can hold conversations in form of posted messages.

Health and Fitness : The internet is now playing a vital role in providing extensive information on health and fitness. Using various medical sites, one can read more about various diseases, their remedies, and precautionary measures.



Disadvantages of the Internet

The internet has several advantages for every individual and it is extremely popular in this modern age. However, it is a tool which must be handled with caution as its misuse can be hazardous. Some of the threats posed by the internet are as follows:

Virus Threat : Computers that are connected to the internet are more prone to virus attacks, which can result in the crashing of the system, data loss, and hardware malfunctioning.



Spamming : It refers to unwanted e-mails that are of commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups. It unnecessarily uses the system's resources and can also be used to spread computer virus or other malicious software.

Theft of Personal Information : The internet is the main source of social evils like privacy, plagiarism, and the privacy of an individual or an organization. One should be careful while handling one's personal information such as name, address, credit card number, etc ., as they can be accessed by hackers or crackers for personal monetary gains. Such elements can also disturb system applications by spreading virus and changing program logics and outputs.



Pornography : This is the major issue posted by the internet. There are many pornographic sites on the internet that can be found easily and can be hazardous to the mental health of the children.




Cyber Terrorism : It causes a serious threat to the world nowadays. Modern terrorist organizations perform targeted attacks on power plants, banks, commercial areas, or buildings of national importance. These can be conducted remotely with the help of a mobile phone and the internet, which

are less expensive than traditional terrorist methods.

Time Wastage : Although the internet provides various services to its users, yet people generally waste time and energy in surfing the net. Spending prolonged time on electronic devices adversely affect our eyesight as well as mental health. This can also result in the loss of our personal interaction with people thus affecting both, our socializing skills and personal relationships.



**KNOW THE FACT**

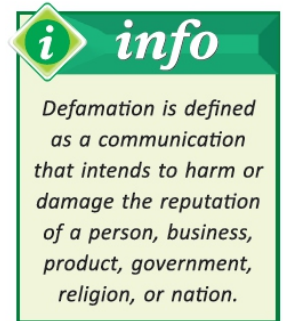
Cyber trafficking refers to the serious crime of selling drugs, weapons, and even human beings over the internet. Traffickers contact their customers through encrypted e-mails and fix their deals at places like Internet cafes in order to sell their illegal substances. Some criminals even build websites for online selling and trade of these harmful commodities.

Computer Ethics

Ethics is a set of moral principles that governs the behavior of a group or an individual. Similarly, computing ethics is a set of procedures, moral principles, and ethical practices that regulate the use of computers. It focuses on ethical implementation and use of computing resources and include new issues that are raised by new technologies. It basically aims at encouraging IT users to be responsible in order to utilize the technology tools judiciously, respect views of others, and acknowledge the rights and properties of other people on the internet.

Given below are some of the common ethical guidelines which should be followed while using a computer:

- Do not use computer technology to steal information or to cause disruption or interference in other users' work.
- Do not spy on another person's computer data.
- Do not contribute to the spread of wrong information using computer technology.
- Avoid buying pirated software. Pay for the software unless it is free.
- Do not use someone else's computer resources without an authorization.
- Do not claim ownership on a work which is output of someone else's intellect.
- Before developing software, think about the social impact it can have.
- Be respectful and courteous with the fellow users while communicating on the internet.



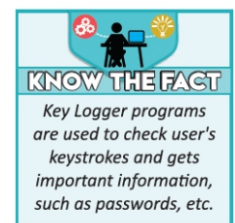
Unethical Practices

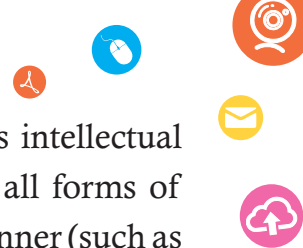
In the following section, we will discuss some of the common unethical practices which are prevalent in the society:

Plagiarism : Plagiarism is the usage or imitation of the language and thoughts of another person projected as one's own original work. It is considered a crime or fraudulent act.

The Merriam-Webster dictionary describes plagiarism as follow:

- To steal and pass off ideas or words of another as one's own.
- To use another's production, without crediting the source.
- To commit literary theft.
- To present new and original, an idea or product derived from an existing source



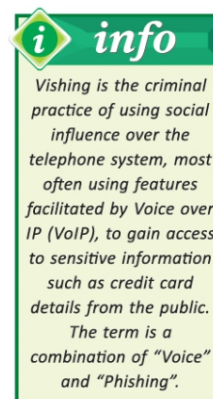


International copyright laws also state, "expression of original idea is considered as intellectual property and is protected by copyright laws", just like original inventions. Almost all forms of expressions fall under the copyright protection as long as they are recorded in some manner (such as a book or a computer file).

Plagiarism has become very easy with technological advances like web searching and cop/paste options. Most critics have linked carelessness, laziness, lack of interest and arrogance as the major reasons of plagiarism.

Measures to Prevent Plagiarism : The simplest way to prevent plagiarism is 'citation'. The process of acknowledging the original writer and the source from where the material has been taken is called 'citation'. It includes the following steps:

- All sources are neither accurate, nor they validate the information as accurate. Therefore, you must specify the source, which informs readers regarding the basis of your ideas and the extent of your research. Citation gives strength to your resource.
- To avoid plagiarism, one can rephrase the matter.
- Use quotation marks around all the quoted words of another person to avoid plagiarism.
- In the education sector, student should be encouraged to present their original and innovative ideas. Even if they wish to refer to resources, they should be made aware of the pattern of references. In this manner, plagiarism can be avoided and students can be motivated to work and bring out their original work.



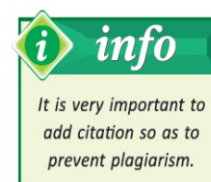
Cyber Bullying :

It is an act of deliberately harming, harassing, or targeting a person by another person using the internet. This includes insulting remarks and threatening messages sent by e-mails, spreading rumors about the person either by emails or social networking sites, posting embarrassing photos and videos to hurt the person, and derogatory remarks against gender, race, religion, or nationality.



Measures to Prevent Cyber Bullying :

- Do not disclose our identity to unknown persons.
- Safeguard your password and all private information from inquisitive peers.
- Do not give bullies any opportunity to misuse the information on the social media platform.





Search the whereabouts of the person you meet online and know about him fully before starting any conversation with him.



Restrict your online profile to be checked by the trusted friends only.

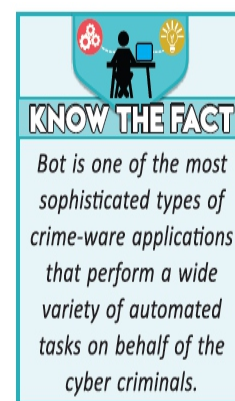
If you are cyber bullied by someone, do not remain silent but take action against cyber bullying. Do not use abusive language, rather block the communication with the cyber bully and share this problem with your parents.

Phishing :

It is an act of sending an email to a user misleading him to believe that it is from trusted person or organization. The user is asked to visit a website in which he is supposed to update or validate his personal details, such as user name, password, credit card details, etc. in this way the operators of the fake website steal your identity and commit crimes in your name. this could damage your reputation and cause heavy financial losses.

Measures to Prevent Phishing :

- Identify suspected phishing emails that come from unrecognized senders. Guard against scam.
- Do not click on links, download files, or open attachments in emails from unknown senders.
- Beware of links in emails that ask for personal details.
- Enhance security of your computer by protecting it with a firewall, spam filters, antivirus, and anti-spyware software.
- Do not divulge personal information over the phone unless you initiate the call. Enter your sensitive data in secured websites only. The URL of a secured website starts with https://: and your browser displays an icon of the closed lock.
- Check your online accounts and banks statements regularly to ensure no unauthorized transaction are made.



Hacking :

Hacking refers to an illegal intrusion into a computer system or network. Hackers are highly technical people who secretly break into computers to steal or sometimes, destroy important data. Hackers not only steal important data but also hack applications and websites to change program logics. Hackers usually tamper with data for unethical purposes, just for an obsession to break the system securities. Although hacking is done without any consent from the user, yet it is not always destructive. Hacking, which is done for a good cause, such as national security, etc., is known as ethical hacking.




Another form of malicious cyber activity is cracking. Crackers are technical people who are experts in breaking into systems, to steal important data, such as financial details, passwords, etc. sometimes they use key loggers for this purpose. Crackers also cause harm to computers by destroying data. Apart from this, they disturb applications by spreading malwares and changing program logics and outputs.

i info
Robotics Kits- In 1998, Lego introduced Mindstorm Robotics kits consisting of standard bricks and building components, motors and sensors, and a programmable brick having the computer that controls the components of the Robot. With the help of these kits, students can develop their Robots to perform specific tasks. Visit – <https://education.lego.com/> to know more details about lego Robot Kits.

Measures to Prevent Hacking :

- Keep your passwords secret and change them periodically.
- Frequently update your operating systems and other software, like antivirus.
- Avoid using open WiFi as it makes easy for hackers to steal the information and download inappropriate content to your system.
- Always make you're of secure websites by looking at the lock sign or https on the address bar. This ensures that the sensitive data which is passed from your device is encrypted, making it difficult for the hacker to decipher the information.
- Always check permissions and authenticity on the apps before installing them. You should also ensure that the apps are not accessing unnecessary information. For example, a drawing app should not have access to your contact list or your network information.
- Never store your credit card information on a website.

**KNOW THE FACT**
A humanoid robot is a robot with its body shape built to resemble the human body. Some humanoid robots also have heads designed to replicate human facial features such as eyes and mouths.

Spamming :

Spams are unwanted bulk emails that come from strange sources. Spams are generally sent in large numbers for commercial advertising. In spamming, millions of copies of same message are sent to email users worldwide. Spam is a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and organize targeted phishing attack. How to identify spam?

- Messages that do not include your email address in the to: or CC: fields are common forms of spam.
- Some spam email can contain offensive language or links to website with inappropriate content.



Measures to Prevent Spamming :

- Install spam filtering/blocking software.
- If you suspect that an email is spam, do not respond, just delete it.
- Reject all instant messages from persons who are not in your contact list.
- Do not click on the URL links within Instant Messenger unless it is received from known source.
- Keep the software and security patches up-to-date.



Individual Right to Privacy :

In this digital era, there has been a significant increase in the use of technology. As the technology is progressing, so are the privacy parameters diminishing. The internet is commonly used for various purposes, such as for personal communication, accessing information on any topic, for financial transactions, etc. the use of the internet can affect the privacy rights and personal data of a person.

Privacy is one of the major concerns in one's life. The right to privacy may be defined as the claim of individuals, groups, or institutes to determine when, how, and to what extent the information about them could be communicated to others. Privacy issues come into picture when personal information is collected, used, and shared without the consent of the authorized person/business concerned. So, certain preventive measures should be taken to avoid infringement of privacy.

Measures to Protect Privacy :

- Be careful while sharing your personal profile on the social networking sites.
- Never share your login details with anyone.
- Delete the sensitive data when not in use.
- Never click on a link sent to you via text or email from a stranger.
- Protect your online privacy by disabling the cookies in the web browser being used. A cookie is a small text file stored on your computer's browser directory that collects the information of your online activity and reports back to the host.
- Install security software like antivirus, anti-spyware, or firewall software to protect your system against intrusions and infections.
- Lock your system when not in use.



Software Piracy :

When software is copied and distributed illegally, it is called software piracy. A license of copyright is required to copy the genuine programs of someone else. You encourage software piracy when:

- You purchase a single licensed copy of the software and load it onto several computers contrary to the license's terms. This is called soft lifting.
- You make unauthorized copies of the copyrighted software and distribute them.
- You install unauthorized copies of software on the hard disks or personal computers.
- You make unauthorized selling of software for temporary use or sell or buy the software CDS/DVDs on rent.



Measures to Prevent Software Piracy :

- Buy a licensed copy of software. Follow the terms and conditions of the license for each software product you purchase. Never make copies and circulate them.
- Purchase software CDs from a reputed seller to ensure that it is genuine. Avoid using illegal CDs given by your friends to listen to your favorite music or watch movies.
- If software is available online, download it directly from the manufacturer's Agreement, User License. otherwise website.
- Register your software to avoid soft lifting.



Intellectual Property Rights :

Intellectual property is a term that refers to the legal property rights of a person over creations of their mind, both, artistic and commercial. Under intellectual property law, owners are granted certain exclusive rights over the use of their creations, such as musical, literary, and artistic works for certain period of time. These rights ensure that the creator's hard work is safe and protected from unauthorized copying and piracy.

Measures to Prevent Intellectual property Rights :

Patent your Inventions : A patent is a right relating to the new inventions that grants the inventor the sole right to make, use, and sell that invention for a specific period of time. The validity period for a patent in India is 20 years from the date of filing of the patent application.

Copyright your Art and Publications : A copyright is a legal right granted by law to the creator for his original work. The rights provided under copyright law prohibit others to create a copy of work, translation of the work and distribution of the work to the public. Legal action can be taken if someone copies the work without the permission of the author or the organization. It covers artistic and literary creations, such as novels, plays, poems, musical compositions, and architectural designs. The copyright of work lasts for more than seventy years, even after the death of its author.

Register your trademark : This protects the brand names, logos, packaging, and other distinctive designs that identify and distinguish the products of one manufacturer or seller from that of others, the validity period for a trademark is ten years and it can be further renewed.

Cyber Crime

A cybercrime is any illegal activity done through internet, e.g., identity theft, where somebody can steal your email id or password and use it to send fake emails containing false information about a product, winning a lottery, etc.



There are also credit card account thefts and internet frauds like ordering goods in others' name, extracting the mobile phone contacts, forgery, imitating documents, currency, and objects other people with bad intentions, harassing others, and mischief mongering by sending threatening messages, all of which come under the jurisdiction of the Indian penal code(IPC). All the above mentioned practices come under cybercrime.

Cybercrimes can be divided into three main categories:

- Crime against an individual person.
- Crime against property.
- Crime against an organization/society.

Safety Measures while using Computer and The Internet

Let us look at the various safety measures which should be undertaken while using a computer or the internet:

- Minors should always surf the internet under the supervision of their parents.
- Parents should decide and suggest age appropriate website to their children.
- To minimize the chances of the attack of hackers and crackers, one should use strong passwords. A strong password consists of at least six characters (more the characters, stronger the password) that are a combination of letters, numbers, and symbols (@, #, \$, &, etc.).
- To avoid losing data privacy while transmitting data from one site to another, encryption can be implemented. Encryption is the process of transforming data into an unreadable code. The result is an encrypted file, which is transferred over the network. At the receiving end, it undergoes a process called decryption which converts the encrypted information into readable form.



- Set up your computer for automatic software and operating system updates to make your system robust.
- Taking regular data backup is the primary and the most reliable method of data protection.
- Ignore unwanted and strange emails and be cautious of attachments, links, and forms in emails that come from unknown people.
- Make use of firewalls. Firewall is a security system that prevents unauthorized people to access your system and network. It can be either hardware or software, or a combination of both. It is implemented on the gateway of a network and follows a specific set of rules defined by user or network administrator. Based on these rules, it controls the incoming and outgoing network traffic.



Quick Look



- The internet is one of the largest information databases.
- It is a global system of inter-connected computer networks that enables the user to share information and various resources with each other. It uses common communication standards and interfaces to provide the physical backbone for many interesting applications.
- Internet has shown dramatic impact on higher education as a growing number of universities offer online courses. Internet is a vast storehouse of information and is also used to publish papers and articles.
- The Internet provides a convenient and economical mode of communication.
- The Internet has brought new opportunities for business to sell goods and services online, which has proven to be beneficial.
- Ecommerce: is the concept used for any type of commercials or business deals that involves the transfer of money across the Globe by using the Internet.
- Media: The Internet has facilitated the media and entertainment industry.
- Social networking: is the latest way to communicate where an individual can connect with friends and strangers on the basis of shared interests or views.
- An Internet forum is online discussion site where like-minded people can hold conversation in form of posted messages.
- The Internet is now playing a vital role in providing extensive information on health and fitness.



- 💡 Ethics is a set of moral principles that governs the behavior of a group or an individual.
- 💡 Plagiarism is the use or imitation of the language and thoughts of another person projected as one's own original work. It is considered a crime or fraudulent act.
The simplest way to prevent is citation.
- 💡 Cyber bullying is an act of deliberately harming, harassing or targeting a person by another person using the Internet.
- 💡 Phishing is an act of sending an e-mail to a user misleading him to believe that it is from a most trusted person or organization.
- 💡 Hacking refers to an illegal intrusion into a computer system or network. Hackers are highly technical people who secretly break into computers to steal information & destroy important data.
- 💡 Spams are unwanted bulk emails that come from strange sources. Spams are generally sent in large numbers for commercial advertising.
- 💡 Cybercrime is an illegal activity done through the Internet. Example: identity theft, where somebody can steal your e-mail ID or password and use it to send fake emails containing false information about a product like winning a lottery, etc.



Section - I

► Objective Type Questions

A. Fill in the blanks with the correct words.

Citation Hacking Computer Ethics Cyber Bullying Intellectual Property

1. A set of procedures, moral principles, and ethical practices that relates to the use of computer, are known as _____.
2. To prevent plagiarism the simplest way is _____.
3. An act of deliberately harassing, harming, or targeting a person by another person using the Internet is called _____.
4. _____ is known as an illegal intrusion into a computer system or network.
5. The legal property rights of a person over creation of his/her mind, both, artistic and commercial are referred to a term called _____.



B. Write T for the true statement and F for the false one:

1. The wanted bulk emails that comes from strange sources are called spams. ☐
2. The usage of limitation of the languages and thoughts of another person and projecting them as once own original work is called hacking. ☐
3. To identify the unsecured website, look at the lock sign RSTP on the address bar . ☐
4. The process of transforming data into unreadable code is called encryption . ☐
5. Foreign unlimited., a patent granted renters the sole right to make, use, and sell that intervention for an unlimited period. ☐

C. Choose the right option:

1. Are the unwanted bulk e-mail that comes from the strain sources?
a. Junk ☐ b. Spam ☐
c. Trash ☐ d. Inbox ☐
2. A small text file stored on the computers browsers directory that collects the information of your online activities and reports back to the text is called
a. Browser ☐ b. Register ☐
c. Cookies ☐ d. Popups ☐
3. Legal rights granted by law to the creator of this original work is known as
a. Trademark ☐ b. Patent ☐
c. Copyright ☐ d. None of these ☐
4. The process of transforming data into an unreadable code is called
a. Decryption ☐ b. Encoding ☐
c. Encryption ☐ d. Decoding ☐
5. An act of sending an e-mail to a user misleading him to believe that it is from a trusted person or organization, in an attempt for malicious purposes is called
a. Hacking ☐ b. Phishing ☐
c. Spamming ☐ d. Cyber Bullying ☐





D. Application Based questions:

1. Neetu have just received an e-mail and by looking at that, she is not able to decide whether the e-mail is a genuine or a spam. Help her in identifying the spam specifying any indicative features.

2. Juhi is preparing for combine defense services exam through the Internet. While surfing the Internet she wants to be sure that the website she's referring to is secured or not. Suggest her the way in which she can identify the same.

Section - II

► Descriptive Type Questions

E. Answer the following question.

1. List the advantages of the Internet.

2. List 5 ethical guidelines which should be followed while using a computer.

3. What is plagiarism? List the steps taken to prevent it.

4. How can you protect your intellectual property rights from getting violated?

5. Write short notes on the following:

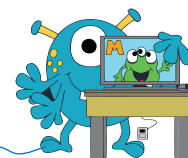
a) Spamming	b) Cybercrime
c) Firewall	d) Software Piracy
e) Hacking	f) Phishing



Activity

TIME

TIME



LAB ACTIVITY

Practice Makes Perfect

Hands-on Activity: Safe Internet Browsing (30 minutes):

Guided Browsing:

- Provide students a list of websites, some safe and some potentially unsafe. Ask students to identify the safe websites and explain why they consider them safe.

Phishing Email Simulation:

- Create a simulated phishing email and ask students to identify the elements that indicate it's a phishing attempt. Discuss the red flags as a class.

Practical Tips and Tools (15 minutes):

Demonstration:

- Demonstrate how to create a strong password and introduce password manager tools for better security.

Safe Searching:

- Teach students how to use safe search filters on popular search engines to avoid inappropriate content.

GROUP DISCUSSION

For Better Clarity



Divide the class into groups and discuss:

- Hackers versus Crackers
- Cyber Bullying versus Cyber Trafficking

PROJECT WORK

For Practicing Ideas



- Make a presentation on unethical practices on the Internet. Make use of effective pictures, audios, and videos clips wherever required.

GROUP DISCUSSION

For Better Clarity



Please explain what is Internet and its advantages and disadvantages

- Explain the Computer Ethics.
- Explain what are cybercrimes?

ONLINE LINKS

For Searching More



- <http://www.esmart.org.au/news/top-10-cyber-safety-tips/>
- <http://www.opencolleges.edu.au/informed/cyber-safety/>
- <http://www.virtuallibrary.info/cybersafety.html/>