Contents

Cyber Ethics

Learning Outcomes

The students will be able to:
- know about computing ethics and unethical practices.
- list online safety measures.
- know about digital footprints.

Hey, KiBo! I found this link on a website. It says that I can win a free iPad if I enter my personal information.

Beware! That's a scam. Never give out personal details online to a stranger.

Oh, I had no idea. Thanks for warning me. I will be more careful and only share personal information with trusted websites or people.

Absolutely! Always be cautious while sharing any personal information online and stay vigilant against scams and frauds.

In this conversation, an example of identity theft is discussed, which is a type of cybercrime. Let us learn more about various types of cybercrimes and how to prevent them.
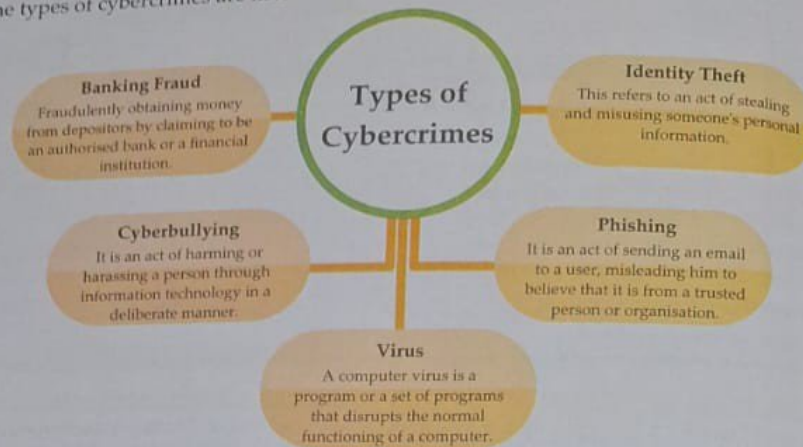
▶ Cybercrime

Cybercrime refers to criminal activities that involve the use of computers, networks, and the internet connections with the intent to cause harm to individuals or their digital devices. Some cybercrimes are executed to damage or disable the victim's computer, while others are used to spread 'malware' (malicious software) to extract secret information from the target computer.

Some types of cybercrimes are listed as follows:

Types of Cybercrimes

Banking Fraud
Fraudulently obtaining money from depositors by claiming to be an authorised bank or a financial institution.

Identity Theft
This refers to an act of stealing and misusing someone's personal information.

Cyberbullying
It is an act of harming or harassing a person through information technology in a deliberate manner.

Phishing
It is an act of sending an email to a user, misleading him to believe that it is from a trusted person or organisation.

Virus
A computer virus is a program or a set of programs that disrupts the normal functioning of a computer.

▶ What is Cyber Ethics?

Information and Communication Technology (ICT) is an integral part of our day-to-day life. The internet and various devices, like computers, mobiles, tabs, etc., are part and parcel of our life. While using the internet, we need to follow certain moral rules, which include honesty, respecting the privacy of others, and property rights. These rules are called cyber ethics. They refers to a set of procedures, moral principles, and ethical practices that regulate the use of a computer and the internet.

▶ Unethical Practices

Unethical practices mean accessing the internet in an illegal manner. Some of the common unethical practices that are prevalent in the society today are discussed as follows:

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 important data or sometimes to destroy it. They 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's 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, is known as **Ethical hacking**.
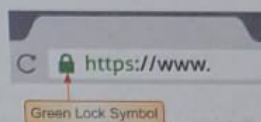
Ways to Prevent Hacking

You can follow the given points to prevent hacking:

◆ Keep your passwords secret and change them periodically.

◆ Update your operating systems and other software, like antivirus, frequently.

◆ Avoid using open wi-fi as it makes it easy for hackers to steal information and download any inappropriate content.

◆ Always make use of secure websites by looking at the green lock sign or https on the address bar. This ensures that the sensitive data that is passed from your device is encrypted, making it difficult for the hacker to decipher the information.

◆ Always check permissions and authenticity of 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 network information.

C 🔒 https://www.

Green Lock Symbol

◆ Never store your credit/debit card information on a website.

Spamming

Spam refers to unwanted bulk emails that come from unknown sources. They are generally sent in large numbers for commercial advertising purposes. Millions of copies of the same message are sent to email users worldwide. Spam is a serious security concern as it can be used to deliver Trojan horses, virus, worms, and spyware, and to organise targeted phishing attacks.

Note

Sometimes, spam attackers keep sending bulk mails till the mail server gets full. This practice is known as **Mail Bombing**.

You can identify a spam with the help of the following:

◆ Messages that do not include your email address in the **To:** or **Cc:** fields are common indications of spam.

◆ Some spams may contain offensive language or links to websites with inappropriate content.

Kips

11

Ways to Prevent Spamming

You can follow the given points to prevent spamming:

- Install spam filtering/blocking software.
- If you suspect that an email is spam, do not respond.
- Reject instant messages from people not in your contact list.
- Do not click on the URL links in instant messenger unless they are from a known source.
- Regularly update both your software and security measures.

Plagiarism

Plagiarism refers to the act of using or imitating the language and thoughts of another person as one's original work. It is considered as a fraudulent act and a violation of **Intellectual Property Act**. Intellectual property refers to the original creations of a person related to intangible categories, like literature, art, design, symbols, logos, etc. Intellectual property rights refer to the legal property rights a person has over their creations of mind, both artistic and commercial.

International Copyright Law also states, "The expression of original ideas is considered as the Intellectual Property and is protected by copyright laws, just like the original inventions". Almost all forms of creative expression are eligible for copyright protection as long as they are recorded in some manner, such as in a book or a computer file.

Ways to Prevent Plagiarism

The simplest way to prevent plagiarism is through proper citation. Acknowledging the original writer and the source from which the material has been taken is essential and is known as citation. It includes the following points:

- Not all sources are reliable or provide accurate information. Therefore, one must specify the source, which informs the readers regarding the basis of one's ideas and the extent of one's research.
- To avoid plagiarism, one can rephrase the material.
- Use quotation marks around the quoted words of another person to avoid plagiarism.
- In the education sector, students should be encouraged to develop and present their original and innovative ideas. Even if they wish to refer to the resources, they should be made aware of the pattern of references. By following these guidelines, plagiarism can be avoided and the students can be motivated to work hard and showcase their originality.

12

Software Piracy

When software is copied and distributed illegally, it is called **software piracy**. A licence or copyright is required to copy the genuine programs of someone else.

You encourage software piracy when:

- you purchase a single licenced copy of the software and load it onto several computers contrary to the licence's terms. This is called **Softlifting**.
- you make unauthorised copies of the copyrighted software and distribute them.
- you install unauthorised copies of software on the hard disks of computers.

Ways to Prevent Software Piracy

Follow the given points to prevent software piracy:

- Buy the licenced copy of the software. Follow the terms and conditions of the licence for each software product you purchase. Never make copies and circulate them.
- Purchase software CDs from a reputed seller to ensure that they are genuine. Avoid using illegal CDs given by your friends to listen to your favourite music or watch movies.
- If a software is available online, download it directly from the manufacturer's website.
- Register your software to avoid softlifting.

Violation of Intellectual Property Rights

Under Intellectual Property Law, the owners are granted certain exclusive rights to ensure that the creator's hard work is safe and protected from unauthorised copying and piracy.

Ways to Protect Intellectual Property Rights

Always try to follow the given points to prevent the misuse of intellectual property:

Patent your Inventions: A patent is a right related 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 the patent application.

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

Kips

13

Register your Trademarks: This protects your brand name's logo, packaging, and other distinctive designs that identify and distinguish the products of one manufacturer or seller from that of the other's. The validity period for a trademark is ten years and can be renewed.

▶ Computer and Internet Safety Measures

Let us look at the various safety measures that 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 websites for their children.

- To minimise the chances of being attacked by hackers and crackers, one should use strong passwords. A strong password must consist of at least eight characters (more the characters, stronger the password) that can be a combination of letters, numbers, and symbols (@, #, $, %, etc.)

- To avoid losing data privacy while transmitting the data from one site to another, encryption can be implemented. **Encryption** is the process of transforming data into unreadable code. The result is an encrypted file that is transferred over the network. At the receiving end, it undergoes a process called **decryption**, which converts the encrypted information into a readable form.

- Set up your computer for automatic software and operating system updates to make it robust.

- Regular data backups are the primary and most reliable method of data protection.

- Ignore unwanted and strange emails and be cautious of the attachments, links, and forms in emails that come from unknown people.

- Make use of firewalls. A **firewall** is a security system that prevents unauthorised people from accessing your system and network. It can be either hardware, software, or a combination of both.

AI Connect

IBM Watson for Cyber Security combines AI and cognitive computing to analyse vast amount of security data, research reports, and threat intelligence. It assists security analysts in detecting and responding to advanced threats.

Cyber Ethics Role Play

- Divide the students of the class into small groups.
- Assign each group a specific cyber ethics topic, from the chapter, that they have learnt to role play. Two scenarios have been given here for reference.
- Give some time for groups to prepare, including discussing the scenario, assigning roles, and deciding how they will perform their role play.
- Allow each group to perform in front of the class.
- After each performance, ask other students of the class to discuss and reflect on the ethical decisions made by the presenting group.

Scenario 1

Some students of class 7 have made a fake online account to harass and spread false information about a classmate. Discuss the feelings of the student who is being cyberbullied. Also, describe the values of respect, empathy, and the consequences of such act.

Scenario 2

Avika has to submit a school project for which she is running short of time. She decided to take help from the internet and found a document that exactly matches with the subject of her project. Discuss the reasons and effects of plagiarism. Also, talk about the importance of original work and academic integrity.

Revisit the Concepts

- Computer ethics is a set of procedures, moral principles, and ethical practices that regulate the use of a computer and the internet.
- Plagiarism refers to the act of using or imitating the language and thoughts of another person and projecting them as one's own original work.

16

KIDS

- Hacking refers to an illegal intrusion into a computer system or network.
- Spam refers to unwanted bulk emails that come from unknown sources.
- The right to privacy may be defined as the claim of individuals, groups, or institutions to determine when, how, and to what extent the information about them could be communicated to others.
- When a software is copied and distributed illegally, it is called software piracy.
- Intellectual property rights refer to the legal property rights of a person over his/her creations of mind, both artistic and commercial.
- A digital footprint is an impression or information about a person that exists on the internet because of his online activity.
- Netiquette refers to being aware of the ethical practices and behaving responsibly and appropriately while using the internet.

Brain Developer

A. Fill in the blanks.

1. _____ refers to a set of procedures, moral principles, and ethical practices that regulates the use of a computer and the internet.

2. The simplest way to prevent plagiarism is through proper _____ .

3. _____ is an act of harming, harassing, or targetting a person using the internet in a deliberate manner.

4. An illegal intrusion into a computer system or network is known as _____ .

Hints
- Hacking
- Cyber Ethics
- Citation
- Cyberbullying

B. State True or False.

1. You can identify the secured websites by looking at the green lock sign or https on the address bar. ☐

2. A digital footprint is also known as a digital dossier. ☐

3. A patent grants the inventors the sole right to make, use, and sell their invention for an unlimited period. ☐

Activity Section

Pihu's father has received the following email:

> **Subject:** XYZ Bank – Account access restricted
>
> Dear Customer
>
> The bank has restricted access to your bank account because the last three login attempts were unsuccessful. To protect your account, all the services have been stopped for the time being.
>
> To fix the problem, you have to login on the portal of the bank http://www.xyzbank.com and update your personal information. You can also click on the link given below:
>
> **Secure Your Account**

Carefully observe the email and answer the following questions:

1. Is the email genuine?

2. Name the unethical practice that is depicted through this email.

3. Name two threats to which the user is exposed.

4. Write two consequences that may occur if the user clicks the link included in the email.

5. Suggest two methods to protect against such unethical practices.

Lab Activity

Design a poster using GIMP on My Safebook and describe various netiquette that should be followed. Take a printout of the poster after designing and paste it in your computer lab.
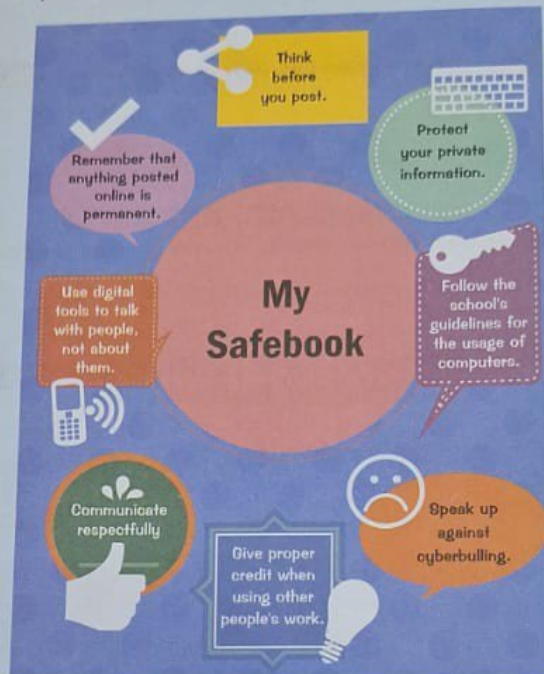
Group Discussion

Discuss the following topic: Digital Footprints and their Types

Project Work

Create a presentation on Unethical Practices Prevalent on the Internet. Make use of relevant pictures, audio, and video clips wherever required.

C. Select the correct option.

1. The unwanted bulk emails that come from unknown sources are called _____ .
   - a. Spam
   - b. Trash
   - c. Draft

2. When a single licenced copy of a software is loaded into many computers contrary to the licence's terms, it is called _____ .
   - a. Softlifting
   - b. Cookie
   - c. Browser

3. A _____ is a legal right granted by law to the creator for his original work.
   - a. Copyright
   - b. Patent
   - c. Trademark

4. _____ is the process of transforming data into an unreadable code.
   - a. Decoding
   - b. Encryption
   - c. Decryption

D. Answer the following questions.

1. List two safety measures you should follow while using the internet.

2. Define spamming. Write any two ways to prevent it.

3. What are digital footprints? Name their two types.

4. How can you prevent software piracy?

18

Act

My Act

Pihu's father has

Subject: XY

Dear Custo

The bank
were unsu
being.

To fix the
update yo

Carefully obs

1. Is the em

2. Name t

3. Name

4. Write

5. Sug

▶ Digital Footprints

In general, footprint is the impression left by a foot or shoe on the ground or a surface. Similarly, a **digital footprint** is an impression or information about a person that exists on the internet because of his online activity. This is the information transmitted online via filling a registration form, email attachments, online shopping, commenting on a social networking site, uploading videos, digital images, etc. A digital footprint is also known as a **digital dossier**.

Digital footprints can be categorised into **active** and **passive** data traces. The active ones are those data traces that a user leaves intentionally. Emails, chats, social networking sites, and blog posts are some of the ways with which a user can create active digital footprints.

Passive data traces, connected to an individual, are generated by others or gathered through the user's online activities without his knowledge. A few activities that create passive data traces include surfing the sites for searching information, online shopping, etc.

▶ Netiquette

The term 'netiquette' is a combination of two terms, 'net' and 'etiquette'. It refers to being aware of the ethical practices, and behaving responsibly and appropriately while using the internet. This includes maintaining your good reputation while accessing social networking sites, representing school groups, playing games online, etc.

Follow the given netiquette while working online:

1. Always be positive in your online behaviour.
2. Respect the privacy of others and let others respect yours.
3. Do not post hurtful messages, mean rumours, or embarassing photos.
4. Be responsible, honest, and truthful.
5. Respect copyright policies and cyber laws.
6. Do not respond to any message that, in any way, makes you uncomfortable. Block them and inform your elders.
7. If you do not agree with the terms and conditions of an online website or an activity, say 'no'.