COMPUTER SECURITY AND ETHICS

Unit 5

SLOs

- Explain the importance of computer security in daily life
- Define various terms related to computer security
- Explain computer crimes by giving real-life examples
- Describe Cyber-Attacks and how to prevent them
- Discuss Cyber- Harassment and what to do in case of becoming a victim
- Explain how to seek help against Cyber-Crime

5.1 COMPUTER SECURITY

The computer has become an important part of our life. We store important data on our computers in the shape of documents, pictures, programs, etc. Therefore, we expect that all our information must remain safe and our computer runs properly without any problem. Few threats can cause problems for our computers. These threats may be different types of viruses or unauthorized use of a computer. To prevent our computer from such threats, we need to abide by computer security. Computer security is the protection against theft or damage to our computer hardware, software and information present on it.

5.1.1 Importance of Computer Security

Computer security is important for our computer's overall health. It keeps our information protected and helps prevent viruses and malware, which allows programs to run quicker and smoother. It safeguards confidential and sensitive information.

The advancement in science and technology has changed the ways we live and carry out day to day activities. We rely on computers and mobile phones to carry out many activities. While using computers and mobile phones we access a lot of information which we do not want to share with others. This information may include our passwords, banking details, contacts, pictures, etc. To protect this information we need to make our devices secured that no one can damage or access this information without our consent.

Computer Security is important as it enables people to perform their work in safe environments. It helps in the execution of essential business processes. Here are a few reasons why computer security should be taken seriously.

5.1.2 Cybercrime:

As communication, trade, and services are relying more on computers and networks, the cybercrimes are growing too. Cybercrime is the crime that is committed through a computer and network. Cybercriminal uses devices to gain unauthorized access to important information. Stealing passwords and important information, hacking social media accounts, accessing anyone else's account and making transactions, committing online frauds are some of the examples of cybercrime. Cybercrime is illegal and also punishable. According to Pakistan's Cybercrime Law, any offender who interrupts the privacy of a person or organization and harms their repute may be sent to jail for three to five years including a heavy fine.

(i) Hackers:

Hacker can be a person who has in-depth knowledge of computer systems, networks, and programs. Hacker maybe someone who uses his or her extensive skills to identify and overcome a network loophole. Hackers constantly seek further knowledge and freely share what they have discovered. Hackers are generally considered as bad people however, hackers can also help us to improve the data and network security. Government and business organizations are now hiring ethical hackers, also known as white hat hackers, to prevent data theft.

(ii) Crackers

Crackers are persons who gain unauthorized access to another system. They bypass passwords or licenses of computer programs, change source code or intentionally breach computer security. They do it with negative intentions. Crackers can also make targeted system unavailable or non-functional. They commit these activities generally for money but they may do it for fame or just for challenge or fun.

5.1.3 Computer Crime in Real Life

As technology is growing the data security has become so crucial. We can be a victim of computer crime at any time. Computer crime can range from an international data security threat to a personal offense. In 2013, hackers managed to hack 1 billion email accounts of the users. Likewise, in 2017, the WannaCry virus attacked the National Health Service in the United Kingdom which made the whole system non-functional for several days. As far as personal offenses are concerned, hacking the social media and mail accounts are so common. There are many genres of computer crime or now called cyber-crimes. Some examples of such crimes in real life are discussed here.

(i) Hacking

Hacking is perhaps the most common crime in the computer world. Hackers can steal our WiFi, email or social media accounts' passwords. Hackers also attack a website and take it down. However, the scope of hacking is much wider. The hackers can also steal sensitive information from government and business organizations, make fraudulent transactions and erase data on the cloud or network computers.

(ii) Credit and Debit Card Scam

Keeping debit or credit cards is a common practice but insecure use of these cards can be dangerous. If a person has information about our debit or credit card he or she can make fraudulent transactions. There are various ways to get this information. One way is through scamming. Scammers set small machines inside an ATM or credit card machine. These machines copy the data which is then misused by the scammers. Debit and credit cards are also secured with PIN codes. User has to keep this code secret otherwise any person can use the card for online shopping and other purposes. All he or she needs to know our credit card number, PIN and security code printed on the back of the cards.

(iii) Phishing

Phishing is a method of trying to gather personal information using false e-mails and websites. In Phishing, perpetrators contact the target

person through email, telephone or text message and pose as a legitimate and trusted individual. He or she asks the target to provide sensitive data such as personally identifiable information, banking and credit card details and passwords for different reasons. The information is then used to access different accounts and can result in identity theft and financial loss.

(iv) Clickjacking

Have you ever seen any video tagged as "OMG? You won't believe what this boy has done!" or did you find a button on a website that asked to click to claim a reward you had never applied for? This is a kind of fraud which is called Clickjacking. Usually, culprits target children or novice internet users to click on a link containing malware or trick them into sharing private information via social media sites.

(v) Cyber Bullying or Harassment

Electronic means like a computer, mobile phone or internet are also used for online bullying or harassment. Harmful bullying behavior can include posting rumors, threats, passing inappropriate remarks, leaking personal information, blackmailing and committing hate speech. The perpetrator does it with the intent to cause harm to the victim. Victims may experience lower self-esteem, intent to commit suicide and a variety of negative emotional responses, including being scared, frustrated, angry and depressed.

5.1.4 Cyber Attack

Cyber-attacks occur when a cybercriminal uses computer or any device to launch attacks to other single or multiple computer networks. The culprit tries to enter in a computer system and network through cracking, scam links, phishing or any other method. Generally cyber-attacks are committed for getting any benefit or causing harm to victim computer, network or websites. A cyber-attack either disables the targeted computer, deletes information or knocks it offline. It may also steal information from the computer or network.

5.1.4 What to do? In Case of Becoming a Victim

The perpetrator of cyber crime always asks to keep his or her contact secret otherwise the victim may face heavy loss. The response of the victim of cyber crime, bullying or harassment is very crucial. There are ways to get rid of such miseries. First thing is to report such incidents to the trusted people that are highly likely parents and teachers.

Fig: 5.1 Cyber Rescue Helpline

The government has also taken measures to curb cybercrimes especially cyber bullying and harassment. In Pakistan, the National Response Centre for Cyber Crimes has been set up to help the victims of cybercrimes. An online complaint can be launched through the form available on the website or help may be sought by calling helpline 9911 which is available 24/7.

SLOs

- Define computer virus and how to prevent them
- Define and differentiate various types of viruses: Malware , Virus, Worm, Adware and Spyware
- Identify that a virus, worm, adware, spyware and Malware can spread through different ways
- Recognize that the antivirus software like Avast, Norton, MacAfee and others can help to safeguard against viruses

5.2 MALWARE

The term malware is the contraction of malicious software. Malware is a broad term that encompasses computer viruses, worms, spyware, adware and others. Malware is a program that is written generally to cause a mess. They can be so dangerous that they can also damage devices. However commonly malware encrypt, steal or delete data, hijack core functions of computing and disturb different activities.

5.2.1 Different Malware

Types of malware can include computer viruses, worms, adware, and spyware.

(i) Computer Virus

A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge. It can also modify other computer programs, insert its own code and change computer settings. Viruses are harmful. They can range from displaying irritating messages to make all the documents inaccessible or even delete them. Viruses generally latch on a host file and when they execute they infect other files or programs. Boot Sector, Resident, Macro Viruses and File Infector are some examples of viruses.

(ii) Worm

A computer worm spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction. It does not need to attach itself to a file or program to cause damage. It can do several malicious tasks, such as dropping other malware, copying itself onto devices physically attached to the affected system, deleting files, and consuming internal storage and memory resources.

(iii) Adware

Adware is advertising-supported software. They present endless ads and pop-up windows that could potentially consume memory and processing resources. Adware can also change the different settings of internet browsers like homepage and default search engine. Normally, these are not as dangerous as other malware. However, Adware annoys the user and slows down the processing. The advertisements produced by adware are sometimes in the form of a pop-up or sometimes in little windows that may not be closed. Adware programs include games, desktop toolbars or utilities. Commonly, adware is web-based and collects web browser data to target advertisements, especially pop-ups.

(iv) Spyware

Spyware is a malware that monitors a device and steals important information about a person or organization without their consent and sends such information to another person or organization. Spyware takes control over a mobile phone or computer without the user's knowledge. They capture information like web browsing history, e-mail messages, usernames and passwords and online payment information. Spyware can come through cookies or even when we install software without reading its terms and conditions. System monitors, cookies trackers, rootkits and key-loggers are few examples of Spyware.

5.2.2 Ways of viruses spread

A computer virus is just like a flu virus. It is designed to spread from one device to another device and can replicate itself. Any device that is infected from a virus can infect other devices. It means that viruses come from outside. How do they come? Here are some ways:

(i) USB Flash Disk and CDs

USB Flash Disks are the most common media to transfer files. An infected computer can spread a virus to a clean USB flash disk that is inserted and likewise, an infected USB can transmit the virus onto a clean computer. The AutoRun function in Windows OS launches installers and other programs automatically when a flash drive or CD is inserted. This action can initiate a virus spreading process onto the computer. Copying infected files from the USB or CD can also infect the computer.

Teacher Note

Teacher should provide the information of viruses like Trojan horses, Rootkit, Backdoors, and Bots. This may be given as an assignment.

(ii) Internet Downloads

Computer viruses also spread through files or software downloads from the Internet. They can be attached to software or files that we download. The viruses come from the internet can also make our computer accessible to hackers. Though, almost every antivirus software provides a shield against malicious downloads,it is highly recommended that the software and files must be downloaded from trusted sources.

(iii) Computer Network

Users must be careful because files picked from a Local Area Network (LAN) may be infected and cause damage to our computer or operating system. The same can happen to transfer files from one mobile device to another mobile device via Bluetooth etc.

(iv) Email Attachments

Email attachments have been a popular medium to spread viruses. Viruses can easily be transferred from one computer to another through email attachments. The infected emails may come from an unknown or fake email address. Perpetrators who spread these viruses use either fake email or change a few letters in a trusted email address. People in our contact list may also send us infected files as they may not be aware of it themselves. Users must check the origin of the email before opening the attached files or clicking any link that is given in the email. Especially spam mails must be checked carefully before clicking on its attachment.

Fig: 5.2 Viruses can spread through emails

5.2.3 Antivirus

Antiviruses are utility software designed to protect computers from any potential threats of data or hardware loss. It is highly recommended that the user must install an antivirus on an operating system like

Windows. Antivirus software works in the background and monitors every software that is running and the emails or data coming from the internet. In case of any suspicious activity, antivirus alerts the user and asks for action. Normally, antivirus tries to clean the files and if not succeeded it quarantines the infected file. This is highly recommended that the user should update the antivirus regularly. Many antivirus software can be found on the internet and most of them are generally free. However, in the free version of antivirus, some advanced features are not available. Paid customers are called premier users and they get advance security features.

The most common antiviruses are:

(i) Avast

Avast is one of the largest security companies in the world. Avast's management claims that they are using next-gen technologies to fight cyber-attacks in real-time. They also claim that Avast has an immense cloud-based machine learning engine that receives a constant stream of data from hundreds of millions of users. This facilitates learning at extraordinary speeds and makes artificial intelligence engine smarter and faster to stop viruses.

Fig: 5.3 Avast Antivirus

(ii) Norton

Norton antivirus has been a popular antivirus utility since 1991. This is a part of a large family of security and other utility software by Symantec Corporation. Norton Antivirus is easy to use, has the configuration options that experts need, comes highly rated by the testing labs and is exactly designed to have the least possible impact on your system performance.

Fig: 5.4 Norton Antivirus

(iii) McAfee

McAfee claims that it provides a combination of antivirus, privacy and identity tools and features. This enables users to stay protected against the latest virus, malware, ransomware and spyware attacks while keeping their identity and privacy protected and personal.

Fig: 5.5 McAfee Antivirus

5.2.4 Safeguard against Malware

Keeping ourselves safe from malware and viruses is mostly in our hands. More than 90% of computers are infected due to the user's mistake. Our computers have caught a virus if they start slowing down, behave unusually, crash during processes or restart several times, show annoying messages and some of our documents disappear or become inaccessible. We must avoid this situation to be created. Some simple measures can prevent our system from malware and viruses.

Fig: 5.6 Schedule scan can safe from data loss

- Install anti-virus software and keep it updated.
- Run scheduled scans regularly with your anti-virus software.
- Keep your operating system updated.
- Do not click on internet links which have unusual labels, images or captions.
- Do not open email attachments or click on hyperlinks from unknown senders.
- Scan USB flash drive, SD cards and mobile phones before opening.
- Use your spam blocking or filtering tools to block unsolicited emails, instant messages and pop-ups.
- Only download files and programs from trusted sources on the internet.
- Never use an open WiFi.

5.2.5 Keeping the Backup of Data

Besides this, we should also take some measures to recover data from any potential loss. Some steps in this regard are:

- Create a system restore point regularly and check if it is not disabled.
- Write important data on CDs or DVDs. Since they are write-protected, they do not catch viruses.
- Have the back-up of important files at more than one place.
- You can also save documents on cloud storage like Google Drive and Microsoft OneDrive.

SLOs

- Describe the authentication mechanism
- List out the different authentication mechanisms
- Differentiate between username and password, personal identification number and biometric authentication mechanisms

5.3 AUHENTICATION MECHANISM

The authentication mechanism is the hardware or software-based mechanism that forces users to prove their identity before accessing data on a device. The process makes sure the only authenticated user gets access to data or devices.

5.3.1 Types of Security Mechanism

There are many ways a computer security system may authenticate a user. Some of them are:

(i) Username and Password:

A username and password are the pair of keywords known by the user. They are presented to the computer to authenticate the user. Usernames and passwords are the default authentication mechanism on

the web today. However, recent large scale computer attacks have made usernames and passwords an unacceptable authentication mechanism. Additional authentication mechanisms are needed to fully authenticate.

(ii) Personal Identification Number

PIN stands for Personal Identification Number. It is a security code for verifying your identity. Similar to a password, your PIN should be kept secret because it allows access to important services such as financial transactions and confidential emails. The PIN provides security when a credit/debit card is lost or stolen because the PIN must be known before making money withdrawal or transfer.

Fig: 5.7 PIN Identification

(iii) Biometric Verification

Unlike authentication processes, biometrics verification makes sure that the real person gets access to the data or device. Biometric authentication relies on the unique biological characteristics of a person. Biometric authentication systems captures data in real-time and compare it with existing data in database. If both samples of the biometric data match, authentication is confirmed. Scanning fingerprints are the most common way of biometric. However, some other advance ways include retinal scans and iris, facial and voice recognitions.

Fig: 5.8 Iris and thumb impression verifications

SLOs

- Explain the importance of professional ethics in computer field
- Define information accuracy
- Explain various types of intellectual property rights: Patents, Copyright and Trademarks
- Explain software piracy and its impacts
- Describe the information privacy
- Discuss plagiarism

5.4 PROFESSIONAL ETHICS IN COMPUTER FIELD

Professional ethics involve the personal and corporate principles and rules that guide behavior within the context of a profession. The role of a professional code of ethics is to clarify values and rules and can be used as a framework for discipline. Computing professionals' actions change the world. To act responsibly, they should reflect upon the wider impacts of their work, consistently supporting the public good. Here are some guiding principles:

- Contribute to society and human well-being, acknowledging that all people are stakeholders in computing.
- Be honest and trustworthy.
- Respect the equipment.
- Avoid causing any harm.
- Be fair and act not to discriminate, bully or harass.
- Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
- Respect privacy and maintain confidentiality.
- Maintain high standards of professional competence, conduct, and ethical practice.
- Create opportunities for other individuals or groups to grow as professionals.
- Manage personnel and resources to enhance the quality of work life.
- Ensure that the public good is the central concern during all professional computing work.
- Access computing and communication resources only when authorized.
- Foster public awareness and understanding of computing, related technologies and their consequences.

5.4.1 Define Information Accuracy

The information accuracy is the type of measurement that assures the information is correct and true. It is also necessary that the information should not be generated from the malicious data. For information accuracy, the data must be from reputable sources.

Fig: 5.9 Ensuring information Accuracy is necessary

In the era of information explosion, we need to be more careful while using or disseminating information. The use of unreliable sources results in inaccurate information. Especially, the accuracy of information shared on social media is often questionable.

5.4.2 Intellectual Property Right

When any person develops software, writes a book or research paper or invents any method or the machine, it becomes the intellectual property of that person. Intellectual property is intangible creations of the human intellect. Just like other property the intellectual property can be stolen. To prevent theft or illegal use or spread of intellectual property, Intellectual Property Right is exercised. Through these rights, intellectual property is protected with the help of copyrights, patents, and trademarks. They allow creators or owners of patents, trademarks or copyrighted works to benefit from their work or investment. Under these rights, no other person or organization can copy or reproduce any other's intellectual property. Intellectual property rights are acclaimed worldwide. In Pakistan, Intellectual Property Organization (IPO) regulates the matters regarding intellectual property rights.

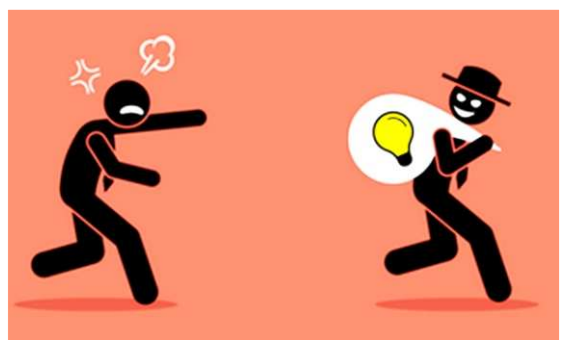

Fig: 5.10 Intellectual Property should be regarded

(i) Patent

A patent is a grant of exclusive rights for an invention to make, use and sell the invention for a limited period, in Pakistan 20 years. Owning a patent gives the patent holder the right to stop someone else from making, using or selling his or her invention without permission. To protect students and scholars, the Higher Education Commission also offers support to get patents registered with Intellectual Property Organization (IPO). The patentable process or invention must be novel, possess inventive steps and can be used in industries.

Fig: 5.11 Patent

(ii) Copyright

Copyright is a legal instrument that provides legal rights to the creator of artwork, literature, or a work that conveys information or ideas. In simple words, copyright is the right of copying. Copyright gives control over how the work is used. Copyright intends to advance the progress of knowledge by giving an author of a work an economic incentive to create new works. The © sign is also often displayed on copyrighted objects.

Fig: 5.12
Copyright

(iii) Trademark

Trademark identifies a product or service and distinguishes it from other products and services. Trademarks are protected by intellectual property rights which identifies that the product or service belongs to a specific organization. It can be an easily recognizable word, phrase, logo, or symbol and often mentioned as TM (Trade Mark). Trademark helps organizations to market their products and services locally and globally. Developing trademarks is creative work and can be done professionally. There are many software available for developing Trademarks.

Fig: 5.13
Trade Marks Registry

5.4.3 Software Piracy

Software piracy is referred to the illegal use, copying or distribution of copyrighted software. Software piracy is a huge threat to the software industry. It causes a significant loss of revenue for developers and vendors. Because of piracy, vendors have fewer resources to devote to research and development of new products. Since they earn less profit, they are forced to pass these costs on to their customers.

Software companies have tried various techniques to stop software piracy but most of them have remained unsuccessful. They applied for copy- protection which demands the user to enter certain keys or credentials. Today, most software require registration which is mainly online. However, these measures could not stop software piracy.

Using pirated software is also risky for users. Aside from the legal consequences of using pirated software, users of pirated software lose some practical benefits as well. Pirated software may not work properly or stop working at any time. Furthermore, pirated software users cannot access customer support, upgrades, technical documentation, training, and bug fixes.

5.4.4 Plagiarism

Plagiarism is presenting someone else's work or ideas as your own without full acknowledgment to the author or conceiver. Academic honesty demands that the users of any ideas, words and data should acknowledge the originators. Plagiarism is unethical and can have serious consequences. Colleges and universities encourage students to submit their original work and cite the ideas and words borrowed from any other sources. Failing to this may cause serious penalties. There are online services to check and fix the plagiarism issues. Academic organizations hire the plagiarism detection service. One of the most used services is Turnitin.

SUMMARY

- Computer security is the protection against damage or theft of computer hardware, its software, and information present on them from threat of viruses or unauthorized use.
- Cybercrime is the crime that is committed through a computer and network.
- Hacker uses his or her skills to identify and overcome a network loophole.
- Crackers are persons who gain unauthorized access to another system.
- Phishing is a method of trying to gather personal information using false e-mails and websites.
- Electronic means like a computer, mobile phone or internet are also used for online bullying or harassment and giving threats.
- Cyber-attack is done when a cybercriminal uses computer or any device to enter or attacks to other single or multiple computer networks.
- Cyber-attack or cyber harassment victim should report to the trusted people and government authorities.
- The malware or malicious software is a broad term that encompasses computer viruses, worms, spyware, adware, and others that is written generally to cause a mess.
- Viruses or malware can be spread from USB Flash Disks and CDs, Internet Downloads, Computer Networks and Email Attachments.
- Antiviruses are utility software designed to protect computers from any potential threats of data or hardware loss from viruses or malware.
- For data safety, the back-up of important files should be made at more than one place.
- The authentication mechanism is the hardware or software-based mechanisms that make sure the only authenticated user gets access to data or devices.
- Professional ethics involve the personal and corporate principles and rules that guide behavior within the context of a profession.
- The information accuracy is the type of measurement that assures the information is correct and true.

- Intellectual property is intangible creations of the human intellect. To prevent theft or illegal use or spread of intellectual property, Intellectual Property Right is exercised. Through these rights, intellectual property is protected with the help of copyrights, patents, and trademarks
- Software piracy is the illegal use, copying or distribution of copyrighted software.
- Plagiarism is presenting someone else's work or ideas without full acknowledgment of the author or conceiver.

A. Choose the right answer:

1. The broad term that encompasses different harmful software is:
   a) Virus b) Malware
   c) Adware d) Spyware

2. The authentication mechanism that only allows the real person to access data or device is:
   a) Username and Password b) PIN
   c) Biometric d) Scan Code

3. Software are mostly protected under:
   a) Patents b) Copyrights
   c) Trademarks d) Logos

4. The professional ethics in computer field is important because:
   a) It is necessary by law.
   b) Violation can cause serious penalties.
   c) It is useful for financial benefits.
   d) It creates healthy and positive work environment.

5. Free Antivirus Software often
   a) Expire after sometimes b) Offer only limited service
   c) Cannot be updated d) Cannot be purchased

6. Copying and pasting some texts from internet without acknowledging the real author is an example of:
   a) Plagiarism
   b) Illegal use of patent
   c) Information Piracy
   d) Copyright Violation

7. Since it does not harm or steal data, the least harmful malware is:
   a) Virus
   b) Adware
   c) Spyware
   d) Trojan

8. The malware that replicates itself and doesn't need to attach with any files is:
   a) Virus
   b) Adware
   c) Spyware
   d) Worm

9. Through which virus spreads?
   a) Email Attachments
   b) Internet Downloads
   c) Flash Disks and Cds
   d) All of them

10. "Click this link and win a $5 voucher at McDonald's". This is an example of:
   a) Scam
   b) Phishing
   c) Clickjacking
   d) Hacking

B. Respond the following:

1. Why is computer security important? Write any three reasons.
2. Explain Cyber Bullying with an example.
3. Why is information accuracy important?
4. What is Ethical Hacking?
5. Your friend has become a victim of cyber harassment. What two advices will you give him or her?
6. Write any two measures to avoid email account hacking.
7. How is software piracy harmful for software developers?
8. Give two examples of phishing.
9. What is an Intellectual Property Right?

10. Differentiate the following on the given criteria.

Criteria	Virus	Worm	Adware	Spyware
Level of danger				
How is it initiated?				
Damage that can be done to data and hardware				
Effect on computer speed				
Means to spread				

C. Match the columns:

S.NO.	A	S.NO.	B
(i)	Presenting someone's ideas as your own without acknowledging the author.	(a)	Adware
(ii)	An advertising software that presents ads & pop-up windows to spread virus.	(b)	Cracker
(iii)	Crime that is committed through a computer system.	(c)	PIN
(iv)	A secretive security code that verifies user's identity.	(d)	Antivirus
(v)	A person that gains unauthorized access to other computers by bypassing passwords.	(f)	Plagiarism
(vi)	A utility software that prevents threats and data loss from a computer.	(e)	Cybercrime

ACTIVITIES

Activity 1:

Organize a poster exhibition in which students suggest measures to the audience how to use the computer and the internet safely. Some focused topics may be:

- Prevent your computers from Viruses and Malware.
- Say no to cyber bullying and harassment.
- Say no to piracy and plagiarism.
- How to cope with cyber crimes?

Activity 2:

During classroom discussion put the following situations before students and discuss what will they do in such a situation? And why?

- You receive a phone call. The caller claims that you have won a huge prize and for delivering the prize they need an advance payment.
- You receive a file from an unknown email address which asks your bank account details or user Email ID and Password.
- While surfing an unknown website, the website demands to access content by providing your Facebook or Gmail account's credentials.

Activity 3:

Make a list of the services that free antivirus software does not offer.

Activity 4:

Search newspapers or internet to find any news about a cyber crime. Specially in which the criminal was caught and punished.

Activity 5:

Thesis and research articles are generally checked through Turnitin which is an Internet-based paid plagiarism detection service. There are other free online services where students can check the plagiarism in their document. Some are:

www.duplichecker.com
www.quetext.com
www.plagscan.com

Write an essay on any topic, and copy and paste some text from internet websites in your essay. Then check plagiarism of your document.