CHAPTER 05

Society, Law and Ethics

In this Chapter...

- Issues Related To Cyber Ethics
- Cyber Safety
- Confidentiality of Information
- Cyber Crime
- Computer Security
- Open Source Software
- Software License
- E-Waste Management
- Digital Society and Netizen

The word cyber ethics refers to a code of safe and responsible behaviour for the Internet community. Practicing good cyber ethics involves understanding the risks of harmful and illegal behaviour online and learn how to protect ourselves, and other Internet users from such behaviour.

It is the study of ethics pertaining to computers, encompassing user behaviour and what computers are programmed to, and how this affects individuals and society. Cyber ethics is the moral, legal and social issues relating to cyber technology. It examines the impact that cyber technology has for social, legal and moral systems. It also evaluates the social policies and laws that have been framed in reply to issues generated by the development and use of cyber technology.

Issues Related to Cyber Ethics

There are many advantages of living in an IT world but on contrary, there are many problems which our society is facing today. The crimes like abduction, fraud etc., have increased leaps and bounds. Hence, there are so many ethical issues as far as IT is concerned.

Some of them are as follows:

1. Plagiarism

The word 'plagiarism' has emerged from a latin word plagiarius, which means **kidnapping**. Plagiarism is an act of copying another person's idea, words or work and pretend that they are our own. The intentions behind plagiarism could be malicious or it could be done accidently like copying data from other's computer without his/her permission and redistributing further. If we talk about the reasons behind plagiarism, then following could be the major factors:

(i) Fear of failure
(ii) Not having enough knowledge
(iii) Being lazy
(iv) Lack of enforcement
(v) Competition
(vi) Lack of management skills

Follow the below given guidelines to avoid plagiarism:

(i) To avoid plagiarism, instead of copying the language of the book as it is, try to put it in your own language/words.
(ii) One should have a clear understanding of plagiarism and its consequences, so that no one can perform it unintentionally.
(iii) If copying someone else's work in our task, word for word, then do not forget enclosing it in quotes and also mention its source.
(iv) Another way is to credit the author has write which was useful for your task and not taking credit for it yourself.

2. Intellectual Property Rights (IPR)

If someone comes out with a new idea, this original idea is that person's intellectual property.

Intellectual Property (IP) is a legal concept, which refers to creations of the mind for which exclusive rights are recognised. Under intellectual property law, owners are

granted certain exclusive rights to a variety of intangible assets such as musical, literary and artistic works, discoveries and inventions, words, phrases, symbols and designs. IPR are the rights given to persons over the creations of their minds. Common types of intellectual property rights include copyright, trademarks, patents, industrial design rights, trade dress and in some jurisdictions trade secrets.

Some of them are as follows:

(i) **Copyright** It includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, painting, photographs and sculptures and architectural designs.

Copyrights are automatically granted to creators and authors. Copyrights law gives the copyright holder a set of rights that they alone can avail legally. It prevents others from copying, using or selling the work. To use other's copyrighted material, one needs to obtain a license from them.

(ii) **Patent** It is usually granted for inventions. Unlike copyright, the inventor needs to apply (file) for patenting the invention. When a patent is granted, the owner gets an exclusive right to prevent others from using, selling, or distributing the protected invention. Patent gives full control to the patentee to decide whether or how the invention can be used by others. Thus, it encourages inventors to share their scientific or technological findings with other. A patent protects an invention for 20 years, after which it can be freely used.

(iii) **Trademark** It includes any visual symbol, word, name, design, slogan, label etc, that distinguish the brand or commercial enterprises.

For example, no company other than Nike can use the Nike brand to sell shoes or clothes. It also prevents others from using a confusingly similar mark, including words or phrases.

Intellectual property rights reserve all the rights of the owner to the information to decide, how much information is to be exchanged shared or distributed.

The protection of intellectual property right of individuals lead to following features.

- It encourages people to create new software as well as helps them to improve the existing applications.
- An environment is provided for the innovative thoughts and technologies.
- Provides the assurity of good returns, people and businesses invest in the national economy.

Violation of IPR

Following are the violation of Intellectual Property Right (IPR):

(i) If a third party were to assume ownership, copy or sell someone's previously copywritten work, that would legally be considered as copyright infringement.

(ii) Copyright law can still be enforced if others try to create simple material from the original source material.

(iii) If a court finds that patent infringement has occurred, the judge will award damages appropriate to compensate for the infringement.

Following are the controls of intellectual property rights:

- Avoid joint ownership
- Get exact match domains
- Safeguard with strong access control

3. Hacking

Hacking means stealing of required information by seeking and exploting weakness in a computer or a computer network.

For gathering required information, a hacker appears with malicious intention and breaks into the owner's system and steals the information illegally.

To prevent hacking, following points are to be used

(i) Create complex passwords.

(ii) Don't give your password to anyone.

(iii) Log out of accounts when you are done with them.

(iv) Make sure you are on an official website when entering password.

4. Piracy

Software piracy means copying of data or computer software without the owner's permission. However, most peoples are aware about piracy and know that it is illegal, yet the piracy is uncontrollable. This is simply the violation of intellectual property rights and right to privacy.

The following are the forms of software piracy:

(i) **Software Counterfeiting** This type of software piracy occurs when fake copies of software are produced in such a way that they appear to be authentic.

(ii) **Softlifting** Purchasing only one licensed copy of a software and distributing and loading it onto multiple systems is called softlifting.

(iii) **Renting** Selling of a software illegally for temporary use as on rent basis is called renting.

(iv) **Hard Disk Loading** Installing an illegal copy of software on the hard disk of a personal computer is called hard disk loading.

(v) **Uploading and Downloading** Creating duplicate copies of the licensed software or uploading and downloading it from the Internet.

In order to stop software piracy, different types of laws as copyright, trademark, patent are used.

Cyber Safety

Cyber safety refers to safety in cyber space. It is a wider concept than the commonly used concept in cyber crime. Cyber safety is the safe and responsible use of Information and Communication Technologies (ICT). Various approaches to cyber safety is founded on

(i) Maintaining a positive approach about the many benefits brought by technologies.

(ii) Encouraging the public to identify the risks associated with ICT.

(iii) Putting in place strategies to minimise and manage risks.

(iv) Recognising the importance of effective teaching and learning programmes.

Safely Browsing the Web

By using a combination of preventative measures and making good choices online you can stay safe when browsing the web. Following are the some precautions for web browsing

Before you Start : Update your Software

Exploiting e-mail and web browsing applications is the most common way hackers and malware try to gain access to devices and your information. Protect yourself before you start browsing the web by make sure that all softwares are up-to-date.

Protect your Web Browser

You can adjust the settings in your web browser to work in a more or less secure way. Most web browsers will give you warnings when they detect you visiting a malicious website. Pay attention to these warnings, they can help to protect you from malware, phishing and identity theft.

Learn more about the Security Settings on your Browser

Settings and security models are different for each browsers, visit the following vendor websites to learn more about the security settings in your browser

(i) Internet Explorer

(ii) Mozilla Firefox

(iii) Google Chrome

(iv) Opera

Identity Theft

It is the act of a person obtaining information illegally about someone else. Thieves try to find information such as full name, middle name, address, date of birth, passwords, phone number, e-mail and credit card numbers. The thief can then use this information to gain access to bank accounts, E-mail, identify themselves as you.

Identity Protection while Using Internet

Your personal identity is important as it defines who you are. Your identity includes your personal information such as name, address, contact information, bank account, credit card numbers and social security numbers should be kept private. We surf the Internet for a variety of reasons from using social media, buying and selling goods etc.. and many more. When we give out our private data to businesses and other internet users such as while filling forms or making payment etc, we trust them to use that information for appropriate purposes.

This is not always the case though and financial and personal data can be used for harmful reasons such as hacking, stalking and identity fraud. Identity fraud is when personal details that have accessed or stolen are used to commit fraudulent acts.

Websites Track You Online in Many Ways

Tracking is generally used by advertising networks to build up detailed profiles for pinpoint ad-targeting even tracking down users for special purpose such as affecting their political choices. The type of information is compiled through your web page usage patterns for tracking you.

This includes the following:

(i) IP Address

The most basic way of identifying you is by your IP address. Your IP address identifies you on the Internet. IP address is a unique address of your device when you connect to Internet. Your computer shares an IP address with the other network devices in your house or office.

From your IP address, a website can determine your rough geographical location. IP addresses can change and are often used by multiple users, so not a good way of tracking a single user over time. An IP address can be combined with other techniques to track your geographical location.

(ii) Cookies and Tracking Scripts

Cookies are small text files that are saved in your web browser when you visit a website. The file might contain your login information, your user preferences, the contents of your online shopping cart and other identifiers. Browser saves the cookies and notes the domain of the website that they belong to. Cookies can also identify you and track your browsing activity across a website.

Cookies can be of the following types:

- **First Party Cookies** By default, first party cookies are allowed in every web browser. First party cookies are user-oriented data packets that are generated and stored locally by the website operator. These are the cookies that store your own login id, passwords for some websites that you frequently visit.
- **Third Party Cookies** Third party cookies are files stored on your computer from advertisers and other parties that have information-sharing agreements with the site you visited. Third party cookies may result in many unwanted advertisements on your web pages.

(iii) HTTP Referrer

When you click the link, your browser loads the web page linked to it and tells the website where you came from.

Fox example, If you clicked a link to an outside website on web page of LIC, the outside website or linked website would see the address of the LIC webpage, you came from. This information is contained in the HTTP referrer header.

The HTTP referrer is also sent when loading content on a web page.

(iv) Super Cookies

A super cookie is a type of browser cookie that is designed to be permanently stored on a user's computer.

It inserted into an HTTP header by an Internet Service Provider (ISP) to collect data about a user's Internet browsing history. Super cookies can be used to collect a wide array of data on user's personal Internet browsing habits including the websites users visit and the time they visit them. These are generally more difficult for users to detect and remove from their devices because they cannot be deleted.

(v) User Agent

The user agent is a browser text string that is given to each website you visit. User agent contains information such as the browser version, compatibility, operating system. Using this data, a website can assess the capabilities of your computer, optimising a page performance and display. Your browser also sends a user agent every time you connect to a website.

Solution to Protect the Identity When Websites Track You Online

All the above things leak your identity information to websites. The most common solution to this is using private browsing or anonymous browsing on Internent.

(i) Private Browsing

This is a privacy feature present in some web browsers that disables web cache, browsing history or any other tracking feature that the browser may have. This allows the user to browse the web without leaving traces such as local data that can later be retrieved.

Private browsing automatically erases your browsing information such as passwords, cookies and history, leaving no trace after you end the session. Private browsing is also known as privacy or incognito mode. There are many other ways to use the Internet without displaying your search history and sharing your data.

- **Incognito Browsing** This is an Internet browser setting that prevents browsing history from being stored. Normally when you visit any web page, text, pictures and cookies required by the page are stored locally on your computer. Incognito mode forgets this data when you close the browser window, or does not store it at all. It is particularly useful if you are entering sensitive data like bank details into the browser, as it can minimise the risk of your information being saved to that computer.
- **Proxy** An Internet proxy is an online computer server that acts as an intermediary between an Internet user and his destination site. Internet users use an Internet Protocol (IP) address to connect to the Internet. This address provides detailed information about the Internet user. When Internet users want to access online information anonymously, they will use an Internet proxy server, which provides a different IP address to the destination website, so that the site does not capture their personal information.
- **Virtual Private Network** (VPN) It is a connection method used to add security and privacy to private and public networks like wi-fi, hotspots and the Internet. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures. However, using a personal VPN is increasingly becoming more popular as more interactions that were previously face-to-face transition to the Internet.

  Privacy is increased with a Virtual Private Network because the user's initial IP address is replaced with one from the Virtual Private Network provider.

Anonymous Browsing

Anonymous browsers allow users to view websites without revealing any personal information like their IP address. One of the most well known anonymous browsers is the Tor browser.

It is an open source piece of software that was originally developed by the united states. It was designed, so that the users could send sensitive information without it being intercepted. Anonymous browsing is popular for two reasons to protect the user's privacy and to bypass blocking applications that would prevent access to websites or parts of sites that the user wants to visit.

Confidentiality of Information

Confidentiality allows authorised users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right or authorise people can infact get it. Access must be restricted to those authorised to view the data. A good example of methods used to ensure confidentiality is an account number or a routing number when online banking. Data encryption is a common method of ensuring confidentiality.

Best practices used to ensure confidentiality are as follows

(i) Use firewall wherever possible.
(ii) Control browsers setting to block tracking.
(iii) Browse privately wherever possible.
(iv) Be careful while posting on Internet.
(v) Ensure safe sites while entering crucial information.
(vi) Carefully handle e-mail.
(vii) Do not give sensitive information on wireless networks.
(viii) Avoid using public computers to make sure the following thinks.
  - Browse privately.
  - Do not save your login details.
  - Never save passwords while using public computer.
  - Disable the feature that store passwords.
  - Properly logout before leaving public computer.
  - Clear history and cookies.

Cyber Crime

Cyber crime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cyber criminals may use computer technology to access personal information, business trade secrets or use the Internet for malicious purposes.

Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as **hackers**.

Cyber crime may also be referred to as computer crime. Computer systems themselves can be the targets of attack, as when a computer virus is introduced into a system to alter or destroy data.

The most serious computer crimes, however, are committed in the banking and financial-service industries, where money, credit and other financial assets are recorded in electronic databases which are transmitted as signals over telephone lines. e.g. illegally transferring large sums of money to their own accounts. Cyber crime involves the use of computer and network in attacking computers and networks as well.

These are the most common cyber crimes acts as follows

(i) Cyber Bullying

This is the use of technology like the Internet, e-mail, cell phones, social media or picture to harass, threaten, embarrass, or target a person. Cyber bullying is one of the most strong crime committed in the virtual world. On the other hand, global leaders are aware of this crime and pass laws and acts that stop the spreading of cyber bullying. Cyber bullying takes place over cyberspace like physical bullying, cyber bullying is aimed at younger people, such as children and teenagers.

(ii) Cyber Trolls or Cyber Trolling

Trolling has become a more common term for any kind of purposeful online abuse on social media sites like twitter or facebook. Cyber trolls refer to offensive or comments posted online targeting people. Trolling is internet slang for a person who intentionally starts arguments or upsets others by posting inflammatory remarks. The single purpose of trolling is angering people. Trolling is the subset of crime of online abuse, trolls are the new generation of cyber criminals who propagate cyber crime of hate.

(iii) Cyber Stalking

It is a form of cyber crime that takes place online when a criminal uses technology to harass or threaten a person or an organisation. It may include monitoring, identity theft, threats or gathering information that may be used to threaten, embarrass or harass.

Cyber stalking is often including by real time or offline stalking. A stalker may be an online stranger or a person whom the target knows. Cyber stalking is a criminal offense under various state anti-stalking, slander and harassment laws.

(iv) Spreading Rumours Online

Spreading rumours on social media also creates panic and confusion among the public. People should stop from posting wrong information on social media, or comments that could hurt others, the official warned that those who did were risking being punished under the cyber crime law.

Spreading rumours online is a cyber crime and is a punishable offense.

(v) Phishing

It is characterised by attempting to fraudulently acquire sensitive information such as passwords, credit cards details etc., by masquerading as a trustworthy person. Victims receive a malicious e-mail or a text messages that imitates a person or an organisation they trust like a bank or a government office.

When the victim opens the e-mail or text, they find a scary message meant to overcome their better judgement by filling them with fear. The message demands that the victim go to a website and take immediate action or risk some sort of consequence.

If users click the link, they are sent to an imitation of a legimate website. From here they are asked to log in with their username and password credentials. If they are innocent enough to comply, the sign on information goes to the attacker, who uses it to steal identities, thieve bank accounts and sell personal information on the black market.

(vi) Ransomware

This is another kind of cyber crime where the attacker gains access to the computer and blocks the user from accessing, usually by encrypting the data. The attacker blackmails the victim to pay for getting access to the data or sometimes threaten to publish personal and sensitive information or photographs unless a ransom is paid.

Ransomware can get downloaded when the users visit any malicious or unsecure websites or download software from doubtful repositories. Some ransomware are sent as email attachments in spam mails. It can also reach our system when we click on a malicious advertisement on the Internet.

Factors in Rise of Cybercrimes

- **Spread of Computers** Computers are becoming more accessible as their cost decreases, leading to a marked growth in their use, particularly in personal and mobile computing. Many home and even business users are unaware of the potential threats from computer crime or may not possess the technical skills to ensure their own security. This greatly increases the risks of cybercrime.
- **Increasing Use of Broadband** These connections allow greater volumes of network traffic, and when coupled with poorly implemented security measures, increase the likelihood of computer attack.
- **Increasing Financial Motivation for Computer Crime** Information security expert, suggest that the motives

behind computer crime have changed. Traditionally, it was motivated by desire for peer recognition and to demonstrate technical skills. However, it is now increasingly financially motivated. The growth of E-commerce with 45% of Internet users participating in some form and the dependence of many aspects of financial life on computers have motivated this shift.

Preventing Cyber Crime

Following points can be considered as safety measures to reduce the risk of cyber crime:

(i) Take a regular backup of important data.
(ii) Use an antivirus software and keep it updated always.
(iii) Do not visit or download anything from untrusted websites.
(iv) Use strong password for web logic and change it periodically. Ignore common words or names in password.
(v) While using someone else's computer, do not allow browser to save password or auto fill data and try to browse in your private browser window.
(vi) Always secure wireless network at home with strong password and regularly change it.
(vii) Always update the system software which includes the Internet browser and other application software.

Computer Security

Computer security is also known as **cyber security** or **IT security**. Computer security is a branch of information technology known as **information security**, which is intended to protect computers. It is the protection of computing systems and the data that they store or access. Most computer security measures involve data encryption and passwords.

Data encryption is the translation of data into a form that is unintelligible without a decode mechanism. A password is secret word or phrase that gives a user access to a particular program or system.

Malware : Threats to Computer Security

Computer systems are vulnerable to many threat that can inflict various types of damage resulting in significant losses.

A **threat** is a potential violation of security and when threat gets executed, it becomes an attack. Those who execute such threats are known as **attackers**.

Malware stands for **malicious software**. It is a broad term that refers to a variety of malicious programs that are used to damage computer system, gather sensitive information, or gain access to private computer systems. Malware is an unwanted software that any unauthorized person wants to run on your computer.

These are also known as **security threats.** It includes computer viruses, worms, trojan horses, rootkits, spyware, adware etc.

Some of them are described below

(i) VIRUS

VIRUS stands for Vital Information Resources Under Seige.

Computer viruses are small programs that can negatively affect your computer. It obtains control of a PC and directs it to perform unusual and often destructive actions.

Virus copy itself and attaches itself to other programs which further spread the infection. The virus can affect or attack any part of the computer software such as the boot block, operating system, system areas, files and application program. On the other hand, it is also true that not all computer problems are caused by computer viruses. This could be caused by other things such as an error (bug) or a misconfiguration of software or hardware.

For example, Bomber, Whale, OneHaff, KoKo, Eliza etc.

Some common types of viruses are as follows

- Resident Virus
- Direct Action Virus
- Overwrite Virus
- Boot Sector Virus
- Macro Virus
- File System Virus
- Polymorphic Virus
- FAT Virus
- Multipartite Virus
- Web Scripting Virus

Effects of Virus

There are many different effects that viruses can have on your computer, depending on the types of virus.

Some viruses can

- monitor what you are doing.
- slow down your computer's performance.
- destroy all data on your local disk.
- affect on computer networks and the connection to Internet.
- increase or decrease memory size.
- display different types of error messages.
- decrease partition size.
- alter PC settings.
- display arrays of annoying advertising.
- extend boot times.
- create more than one partitions.

(ii) Worms

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause atleast some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify

files on a targeted computer. Worms are hard to detect because they are invisible files.

For example, Bagle, I love you, Morris, Nimda etc.

(iii) Trojan

A Trojan or **Trojan Horse** is a non-self-replicating type of malware which appears to perform a desirable function but instead facilitates unauthorized access to the user's computer system. Trojans do not attempt to inject themselves into other files like a computer virus. Trojan horses may steal information, or harm their host computer systems. Trojans may use drive-by downloads or install via online games or Internet-driven applications in order to reach target computers. Unlike viruses, Trojan horses do not replicate themselves.

For example, Beast, Sub7.Zeus, ZeroAccess Rootkit etc.

(iv) Spyware

It is a program which is installed on a computer system to spy on the system owner's activity and collects all the information which is misused afterwards. It tracks the user's behaviour and reports back to a central source. These are used for either legal or illegal purpose. Spyware can transmit personal information to another person's computer over the Internet.

Spyware can harm you in many ways such as

- Malware will log your keystrokes.
- Steal your passwords.
- Observe your browsing choices.
- Spawn pop-up windows.
- Send your targeted e-mail.
- Redirect your web browser to phishing pages.
- Report your personal information to distant servers.
- Can alter your computer settings (like web browser home page settings or the placement of your desktop icons).
- Can affect the performance of your computer system.

  For example, CoolWeb Search, FinFisher, Zango, Zlob Trojan, Keyloggers etc.

Symptoms of a Malware Attack

There are list of symptoms of malware attack which indicate that your system is infected with a computer malware.

Some primary symptoms are as follows

- Odd messages displaying on the screen.
- Some files are missing.
- System runs slower.
- PC crashes and restart again and again.
- Drives are not accessible.
- Anti-virus software will not run or installed.
- Unexpected sound or music plays.
- The mouse pointer changes its graphic.
- Receive strange e-mails containing odd attachments or viruses.
- PC starts performing functions like opening or closing windows, running programs on its own.

Solutions to Computer Security Threats

To safe the computer system from unauthorized access and threats, it is necessary to design some safeguards that handles these threats efficiently.

Some safeguards (or solutions) to protect a computer system from accidental access, are described below

(i) Antivirus (Virus Cleaner)

It is an utility program or set of programs that are designed to prevent, search, detect and remove viruses and other malicious programs like worms, trojans, adware and many more. It is very important to use an antivirus software for users, who use Internet because a computer without antivirus may get infected within few minutes. e.g. Symantec, Norton, Avg, McAfee, Quick Heal etc.

(ii) Digital Certificate

It is the attachment to an electronic message used for security purposes. The common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. It provides a means of proving your identity in electronic transactions. The digital certificate contains information about whom the certificate was issued to, as well as the **certifying authority** that issued it.

(iii) Digital Signature

A digital signature authenticates electronic documents in a similar manner a handwritten signature authenticates printed documents. It is an electronic form of a signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and also ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable and cannot be imitated by someone else. Also, the signer of a document cannot later disown it by claiming that the signature was fake.

(iv) Firewall

A firewall can either be software-based or hardware-based and is used to help keep a network secure.

Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set.

A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external (inter) network, such as the Internet, that is not assumed to be secure and trusted.

There are two forms of firewall

- **Hardware (External) Firewall** It provides protection to a local network. It is physical device that sits between the computer and the Internet. Hardware firewall requires quite a bit of work to fully configure.

These may range from a simple router to a proxy server that directs all traffic to a server elsewhere on the Internet before sending or taking data from a computer or a network.

- **Software (Internal) Firewall** It installed directly into the computer as programs. Once installed, these firewalls activate themselves and set up with relative ease.

(v) Password

A password is a secret word or a string of characters used for user authentication to prove identity or access approval to gain access to a resource, which should be kept secret from those who are not allowed to get access.

In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, ATMs etc.

A password is typically somewhere between 4 to 16 characters, depending on how the computer system is set up.

When a password is entered, the computer system is careful not to display the characters on the display screen, in case others might see it.

There are two common modes of password as follows

- **Weak Password** Easily remember just like names, birth dates, phone number etc.
- **Strong Password** Difficult to break and a combination of alphabets and symbols.

Some Other Threats to Computer Security

Adware These are the kind of unwanted programs which appear on your computer as advertisement. They harm the network bandwidth, slow down the speed of your computer, change the home page of your computer and reduce the stability and usability of your system.

Eavesdropping In computer security, this is defined as the unauthorised interception of a conversation, communication or digital transmission in real time. The various forms of communication include phone calls, E-mails, instant messages or any other Internet service.

Spam It is the abuse of messaging systems to send unsolicited bulk messages in the form of E-mails. It is a subset of electronic spam involving nearly identical messages sent to numerous recipients by E-mails.

Open Source Software

Open source refers to something that can be modified and shared as its designed publicly accessible.

Open Source Software (OSS) is any computer software that is distributed with its source code available for modification.

Examples of Open Source Software are Linux, Unix, MySQL etc.

To be considered as open source software by the software development industry, certain criteria must be met as follows

(i) Software must be available free or at a low cost.
(ii) Source code must be included.
(iii) Anyone must be allowed to modify the source code.
(iv) Modified versions can be redistributed.

Criteria for the Distribution of OSS

Open source software is normally distributed with the source code under an open source license.

The distribution terms of open source software must comply with the following criteria :

(i) **Free Redistribution** The license shall not restrict any party from selling or giving away the software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.

(ii) **Source Code** The program must include source code and allows distribution with source code as well as a compiled form. The source code must be in the preferred form in which a programmer would modify the program.

(iii) **Integrity of The Author's Source Code** The license may restrict source code from being distributed in modified form only if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time.

Software License

A software license is a license agreement that gives an individual, a company or an organisation permission to use a software program. It typically provides end users with the right to one or more copies of the software without violating copyrights. The license also defines the responsibilities of the parties entering into the license agreement and may impose restrictions on how the software can be used.

Types of Software License

Software licenses typically are the either proprietary or free and open source. The distinguishing feature being the terms under which users may redistribute or copy the software for future development or use.

(i) Proprietary Software License

The hallmark of proprietary software license is that the software publisher grants the use of one or more copies of software under the End-User License Agreement (EULA), but ownership of those copies remains with the software publisher. This feature of proprietary software licenses means that certain rights regarding the software are reserved by the software publisher.

In other words, without acceptance of the license, the end user may not use the software at all. One example of such a proprietary software license is the license for Microsoft Windows.

Sometimes one can choose between perpetual (permanent) and annual license. For perpetual licenses, one year of

maintenance is often required, but maintenance renewals are discounted. For annual licenses, there is no renewal, a new license must be purchased after expiration.

(ii) Free and Open Source Software License

It refers to the software that users can safely run, adopt and redistribute without legal restraint. Open source software refers to freedom to use, share and/or modify the source code and allow copies to other users. Open source softwares are further classified into Permissive license and Copyleft license.

- **Permissive License** Those with the aim to have minimal requirements about how the software can be redistributed are called permissive license. It permits using copying, modifying, merging, publishing, selling and distribution without the source code. Examples of permissive license are as follows:

  (a) **MIT License** It is a permissive free software license originating at the Massachusetts Institute of Technology (MIT) in the late 1980s.

  It is compatible because it can be re-licensed under other licenses. MIT license basically allows developers to modify source code according to their preferences. The MIT license also permits reuse within proprietary software, provided that either all copies of the licensed software include a copy of the MIT license terms and the copyright notice.

  (b) **BSD License** It represents a family of permissive free software licenses that have fewer restrictions on distribution compared to other free software licenses. There are two important versions of BSD license.

  (c) **Modified BSD License or 3-clause License** It allows unlimited redistribution for any purpose as long as its copyright notices and the license's disclaimers of warranty are maintained.

  The license also contains a clause restricting use of the names of contributors for support of a derived work without specific permission.

  (d) **Simplified BSD License or 2-clause License** The simplified BSD license is different from new BSD license (3-clause) license in the sense that it omits the non-endorsement clause.

  (e) **Apache License** It is a permissive free software license written by the Apache Software Foundation (ASF). It allows users to use the software for any purpose to distribute it, to modify it and to distribute modified versions of the software under the terms of the license. Through open source code, apache encourages users to voluntarily improve the design of the software.

- **Copyleft License** Copyleft is a method for making a software program free, while requiring that all modified and extended versions of the program also be free and released under the same terms and conditions. When an open source software project is published with a copyleft license, other developers have the right to use, modify and share the work as long as the reciprocity obligation is maintained.

  Examples of copyleft license are as follows:

  (a) **GNU GPL (General Public License)** GPL is a copyleft license. This means that any software is written based on any GPL component must be released as an open source. The result is any software that uses any GPL open source component is required to release its full source code and all of the rights to modify and distribute the entire code. The GPL is based on four freedom to use the source code for any purpose, the freedom to make modification, the freedom to share the source code with anyone and the freedom to share changes.

  (b) **CC (Creative Common) License** CC is an internationally active non-profit organisation that provides free licenses for creators to use when making their source code available to the public. These licenses help the creator to give permission for others to use the source code in advance under certain conditions.

  Every CC license allows you to :

  - Copy the source code (e.g. download, upload etc.)
  - Distribute the source code (e.g. provide copies of the code)
  - Communicate the source code (e.g. make the code available online)

  (c) **GNU Lesser General Public License (LGPL)** It is a free software license published by the Free Software Foundation (FSF).

  The license allows developers and companies to use and integrate a software component released under the LGPL into their own software without being required by the terms of a strong copyleft license to release the source code of their own components. One feature of LGPL is the permission to relicense under the GPL any piece of software which is received under the LGPL. This feature allows for direct reuse of LGPLed code in GPLed libraries and applications.

Open Data

The data that is freely available to everyone to use and republish according to their own requirement, without any restrictions is called open data.

Open data includes non-textual material such as mathematical and scientific formulae, bioscience, biodiversity etc.

Privacy

The right to privacy refers to the concept that one's personal information to be protected from public scruting. Privacy is related to the personal information and, the major issues

regarding an individual's right to privacy in the context of computing information related to the following main information functions :

(i) Collecting information
(ii) Storing information
(iii) Distributing information

The right to privacy also involves decisions related to queries like-what information about an individual or other person must revealed to others, under what conditions and with what safety measures? Hence, the risk of invading other's privacy is becoming more serious, as the role of information technology in decision making is increasing day-by-day. With the increase the use of Internet as the means of information transmission, Internet can affect the privacy rights of a person. A person's Internet usage and transaction done by him/her generates a large amount of information, which provides insights into that person's interests and other vital information.

But, in order to preserve personal information, it is suggested not to use computers to gather, save or distribute information that exclusively belongs to some other person.

How to Safeguard User Privacy?

To ensure that the user privacy is not compromised, following measures must be taken:

(i) The merchant or the seller must clearly state about how the user data will be used, in the terms and conditions of its site application.
(ii) The merchant or seller must ensure that the user has gone through the terms and conditions given on its site application prior for making any transactions.
(iii) The merchant must assure the user about data safety by implementing proper safety and security measures such as https protocol and other security mechanism so that users' data is safe from hackers too.
(iv) The user must go through the terms and conditions of the seller/merchant site before providing any sensitive information and make sure that the site is a safe by checking https protocol and padlock sign etc.

Privacy Laws

Privacy laws refer to the laws that deal with the regulation, storing and using of personally identifiable information, personal healthcare information and financial information of individuals, which can be collected by governments, public or private organisations or other individuals. Privacy laws are considered within the context of an individual's privacy rights or within reasonable expectation of privacy.

Information Technology Act, 2000 has two sections relating to privacy as

(i) **Section 43A** It deals with implementation of reasonable security practices for sensitive personal data or information and provides for compensation to a person affected by wrongful loss or wrongful gain.

(ii) **Section 72A** It provides for imprisonment for a period of upto 3 years or/and a fine of upto ₹ 5,00,000 to a person who causes wrongful loss or wrongful gain by disclosing personal information about another person while providing services under the terms of lawful contract.

IT (Information Technology)

Information technology is application of computers and telecommunication equipment store, retrieve, transmit and manipulate data. IT is generally not used in reference to personal or home computing and networking. IT refers to anything related to computing technology, such as networking, hardware, software, Internet or the people that work with these technologies.

Importance of Information Technology in various Fields

Each field has been changed using information technology below:

(i) In Business

Using IT, businesses have the ability to view changes in the global markets far faster than they usually do. They purchase software package and hardware that helps them get their job done. Information technology has allowed businesses to keep up with the supply and demand as consumes grow more anxious to have their items instantly.

(ii) In Education

With so much focus placed on education, it can sometimes be difficult to hold a job and still get the training needed to get a better job. IT plays a key role in students being able to keep their jobs and go to school. Information technology is helping to prevent more high school and college dropouts as well.

(iii) In Finance

IT might just working its hardest with Internet transactions. As more transactions are done, the Internet requires more networks, more computers and more security programs to keep its consumers safe. Information technology has also made it faster and easier than ever to send or receive money. This allows lenders, insurance companies and businesses to run a quick credit check on you making it far easier to open credit.

(iv) In Healthcare

Improvements in information technology have allowed for great reform in healthcare. You can read about the privacy of your online medical records from HHS. Learn about changes in the healthcare industry with an online class.

(v) In Security

With so many transactions done online and so much information available online, it is important to keep all of that safe. IT makes it possible for your online data to stay secure until accessed by the proper channels. Information technology hides your personal digital data away and the only

way it can be accessed is by companies who have permission from you.

Introduction to IT Act 2000

The Information Technology Act, 2000 (also known as IT Act or IT A-2000) is an Act of the Indian Parliament notified on 17 October 2000. An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication. Commonly referred to as "electronic commerce", which involves the use of alternatives to paper-based method, of communication and storage of information, to facilitate electronic filing of documents with the government agencies.

The origin at Act contained 94 sections, divided in 19 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.

The formations of controller of Certifying Authorities was directed by the Act, to regulation issuing of digital signatures. It also defined cyber crimes and prescribed penalties for them. It also established a cyber Appellate Tribunal to resolve disputes rising from this new law.

Amendments

A major amendment was made in 2008. It introduced the section 66A which penalised sending of "offensive message". It also introduced the section 69, which gave authorities the power of interception or monitoring or decryption of any information through any computer resource. It also introduced penalties for child porn, cyber terrorism and voyeurism. It was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by Rajya Sabha. It was signed by the President of 5 February 2009.

Objectives of IT Act

(i) To stop computer crime and protect privacy of Internet users.
(ii) To make more power to IPO, RBI and Indian evidence Act for restricting electronic crime.
(iii) To give legal recognition for keeping books of accounts by bankers and other companies in electronic form.
(iv) To give legal recognition to digital signature for accepting any agreement *via* computer.
(v) To provide facility of filling document online relating to school admission or registration in employment exchange.
(vi) To give legal recognition to any transaction which is done by electronic way or use of Internet.

Scope of IT Act

(i) IT Act 2000 is not applicable on the attestation for making will of any body. Physical attestation by two witnesses is must.
(ii) Attestation for giving power of attorney of property is not possible *via* electronic record.
(iii) A contract of sale of any immovable property.
(iv) IT Act 2000 is not applicable on the attestation for creating trust *via* electronic way. Physical attestation is must.

Features of IT Act 2000

(i) It helps to promote E-commerce.
(ii) It includes high penalty for cyber crime.
(iii) It provides filing online forms.
(iv) It enhances the corporate business.

Technology and Society

ICT (Information and Communication Technology) are general purpose technologies whose value and impact arise primarily from their use in other economic and social sectors. Three capabilities are especially important for economic and social development as

(i) Enable greater efficiency in economic and social processes.
(ii) Enhance the effectiveness of co-operation between stake holders.
(iii) Increase the volume and range of information available to people, businesses and governments.

Societal Issues by Technology

(i) **Lack of social skills** Frequency of interacting personally has been reduced much thus kids and teenagers are deprived of basic social manner.
(ii) **Poor sleeping habit** Endorsing online activities have affected the sleeping pattern of people.
(iii) **Addiction** Addiction of technology is not less than the drug addiction.
(iv) **Depression** Dependence on technology and less interaction with fellow human beings can lead to depression.
(v) **Lack of privacy** People are opening up their private space by giving their information on social sites giving rise to criminal activities.

Cultural Changes Induced by Technology

(i) **Online shopping** Use of online shopping has changed the culture of going out to the market and buying goods.
(ii) **Home delivery of foods** Online home delivery of foods have changed the culture of going out for a dinner or lunch with family and also the culture of home cooked food.
(iii) **Social media** Social media has changed the culture of going to a friends place to have a chitchat.