NATIONAL INSTITUTE OF ELECTRONICS AND INFORMATION TECHNOLOGY
Sumit Complex, A-1/9, Vibhuti Khand, Gomti Nagar, Lucknow,

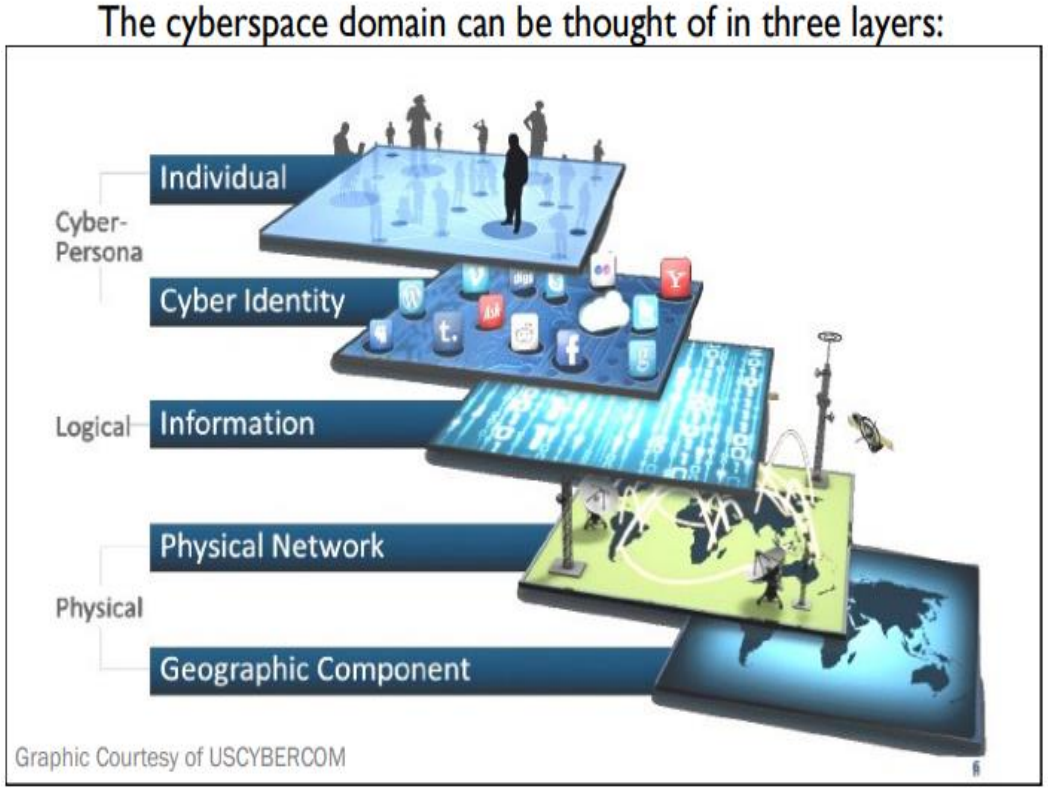
Cyber Security Awareness Program
29.08.2022 to 02.09.2022

Index

Introduction to Cyber space

A place that is not real, where electronic messages exist while they are being sent from one computer to another

In other words, we can say internet is a set of computer networks that communicate using the internet protocol whereas cyberspace is a world of information through the internet.



Introduction to Cyber space

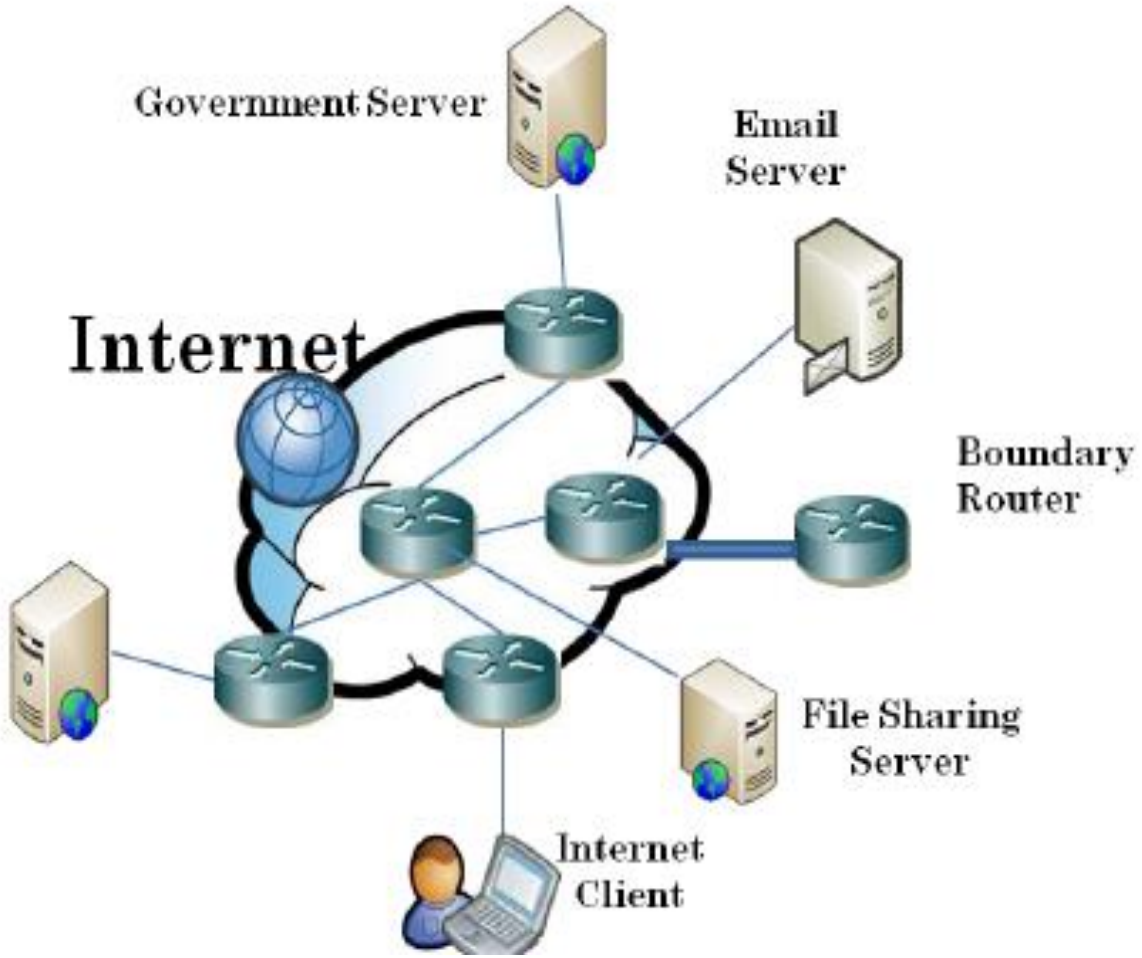
Cyber-persona layer: comprised of individuals and entities on the network. An individual (e.g. "Jane Smith") is digitally represented through his/her cyber identities.

Logical network layer: comprised of the code—"the 1s and 0s"—that conveys information; but is not tied to a specific individual, path, or node.

Physical network layer: comprised of the geographic and physical network components. This includes the location of where elements of the network reside and is comprised of the hardware, systems software, and infrastructure that support the network (routers, switches, transmitters).

What is Internet

- It is an international *network of networks* that consists of millions of private, public, academic, business, and government packet switched networks, linked by a broad array of electronic, wireless, and optical networking technologies.



Features of Internet

- **Email:** Email is now an essential communication tools in today's world and you can send and receive instant electronic messages, which work like writing letters. Your messages are delivered directly to people anywhere in the world. Email is free, fast and very cheap when compared to telephone, fax and postal services.
- **Information:** Information is the major advantage Internet is offering. There is a vast amount of information available on the Internet every subject, ranging from government law and services, Business fairs and conferences, market information, new ideas and technical support.
- **Online Chat:** You can access many chat rooms on the web that can be used to meet new people, make new friends, as well as to stay in touch with parents, friends and old friends.
- **Services:** Many services are provided on the Internet like net banking, job searching, purchasing tickets, hotel reservations, guidance services on array of topics engulfing every aspect of life.

Features of Internet

- **E-commerce:** You can shop online using some retail sites available on the Internet that can be used to look for products as well as buy them using your debit, credit card, Internet banking and Cash Wallet option available on the website's provided.
- **Entertainment:** Internet provides facility to access wide range of Audio/Video songs, plays films. Many of which can be downloaded. One such popular website is YouTube.
- **Software Downloads:** You can freely download innumerable, software's like utilities, games, music, videos, movies, etc. from the Internet.

Limitations of Internet

Exposing your Computer to Unwanted Software

Usually, many peer-to-peer file sharing programs do not employ good security or access control. If users are not familiar with the programs or improper configuration of the settings, it will be dangerous for all the contents stored in user's hard disk to be exposed to other users.

Contracting Computer Viruses

Besides, the computers of P2P software users can easily contract computer viruses especially when the file downloaded is from an unknown source. Moreover, these P2P programs may also contain viruses and worms, which prevent users' computers from functioning properly.

Infringing Copyright

Many copyright laws infringing copies of entertainment files e.g. MP3 Music files, VCD video files etc. and software are often shared by P2P software.

The act of unauthorized uploading of a copyright works for others to download may attract civil or even criminal sanctions. Unauthorized downloading of copyright works entails civil liability.

Children privacy can be compromised in certain online activities:

- On filling forms for various surveys, contests, download games on commercial or free web sites.
- Giving details about personal information when registering for e-mail access, Chat access.
- Providing information when registering for free game downloads.
- Providing information when registering for social networking web sites.

What is Cyber Security

Cybersecurity is **the practice of protecting systems, networks, and programs from digital attacks**. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Cybersecurity can be categorized into five distinct types:

- Critical infrastructure security.
- Application security.
- Network security.
- Cloud security.
- Internet of Things (IoT) security.

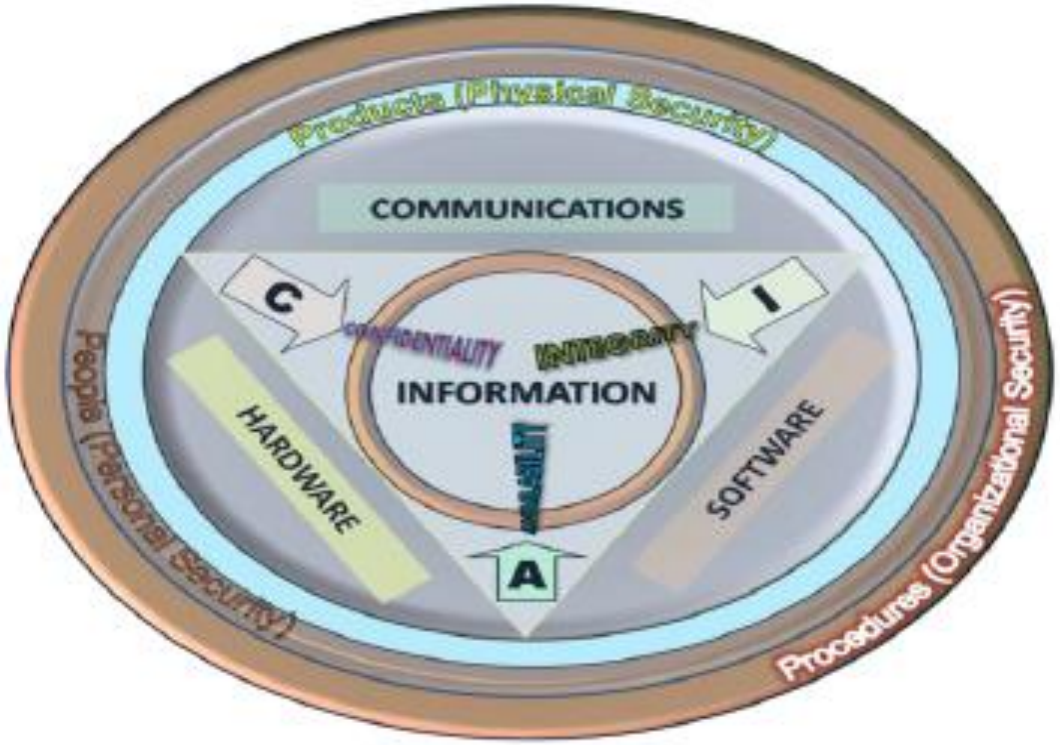
Importance of Cyber Security

- Advanced technologies have changed the modern way of life. The internet provides us with many benefits. Be it communicating with friends, searching for information, doing banking transactions, availing online services, finding job, finding life partner or even running entire businesses. The internet touches almost all aspects of our lives. However, it also makes us vulnerable to a wide range of threats.
- New and powerful cyber-attacks are striking the internet regularly. A minor lapse in managing our digital lives can open the door to cyber criminals. Cyber criminals can steal our money or damage our reputation. According to a study by a leading industry research organization, 90% of all cyber-attacks are caused by human negligence. Therefore, cyber security awareness is important for everyone today.
- We must be vigilant while making use of technology to reduce the risk of cyber threats

Basic Principles of Cyber Security

A security system has to provide services for information security. These services are called information security services.

- Confidentiality
- Integrity
- Availability



CONFIDENTIALITY:

Confidentiality service is to ensure the secrecy of information. Only authorized users should be able to gain access to the information. Confidentiality has to be ensured for information stored in the computers in the form of files. Also, while this information is being transmitted through physical means or through a network, it should be ensured that the information reaches only the authorized users.

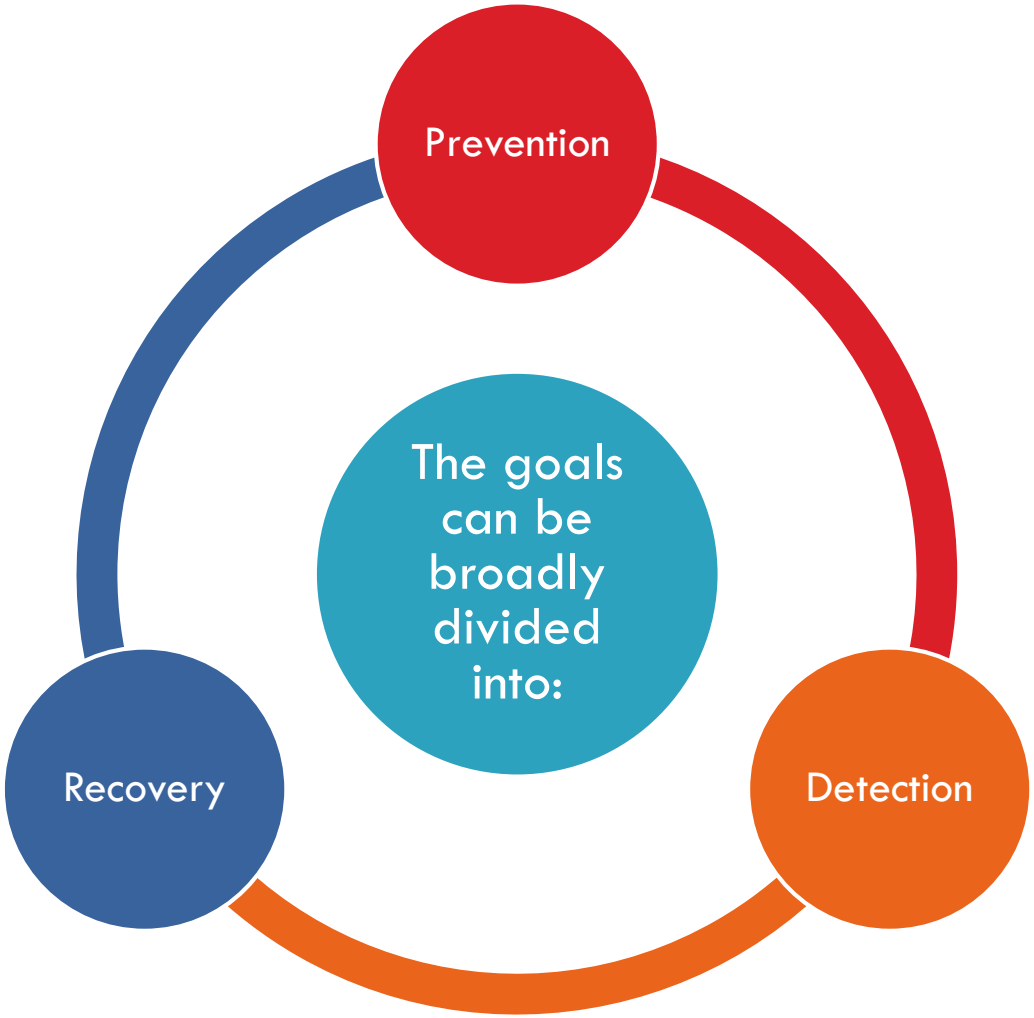
INTEGRITY:

Integrity service is to ensure correctness of information. If A sends some information to B, A should be sure that the information received by B is same as that has been sent. B also should be sure that the information sent by A is same as that has been received.

AVAILABILITY:

The information infrastructure such as the computers and networks are valuable assets for any organization. If the authorized users are unable to access these computers, then it is a denial-of-service attack. Availability service ensures that the information infrastructure is available to the authorized users.

Goals of Cyber Security



Goals of Cyber Security

Prevention:

As we all know, prevention is better than cure. But then, it is not always possible to take enough measures to ensure that there will be no attacks. However, the security system should aim to ensure that a possible attack will fail. This is prevention. Some of the examples for preventive measures are: protecting the systems through passwords

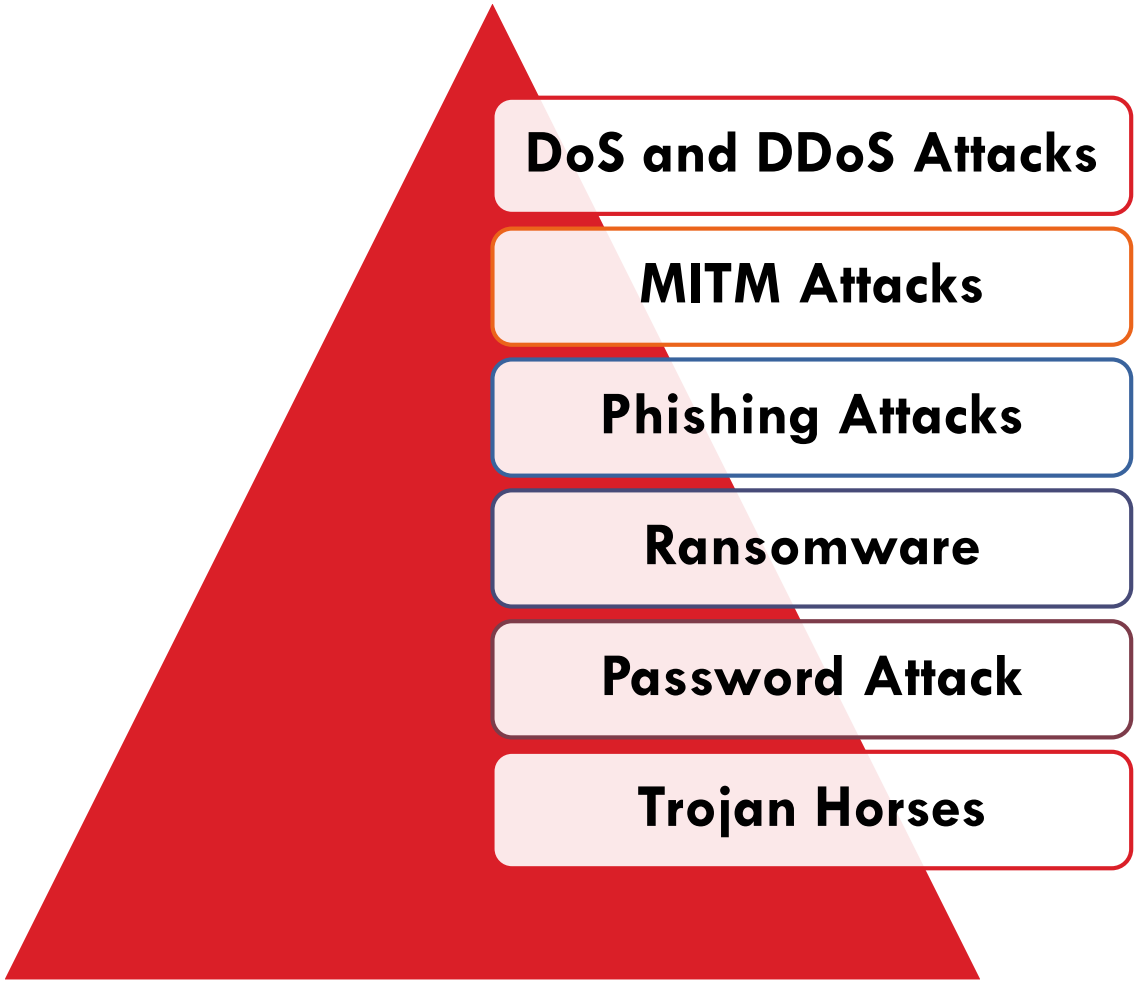
Detection:

Another goal for security is detection. This goal is to devise mechanisms to find out that an attack is taking place or an attack has taken place. If the attack is discovered while it is taking place, the damage being done can be monitored and if possible the attack can be stopped. If the attack has already taken place, the damage that has been done should be detected.

Recovery:

The third goal of security is recovery i.e., to repair the damage done by an attack. An examples of recovery is: when a file is deleted through an attack, to restore that file from the backup. Of course, the underlying assumption is that you have a backup. So, the security system should work out a backup policy.

Common Attacks



DoS and DDoS Attacks

DoS

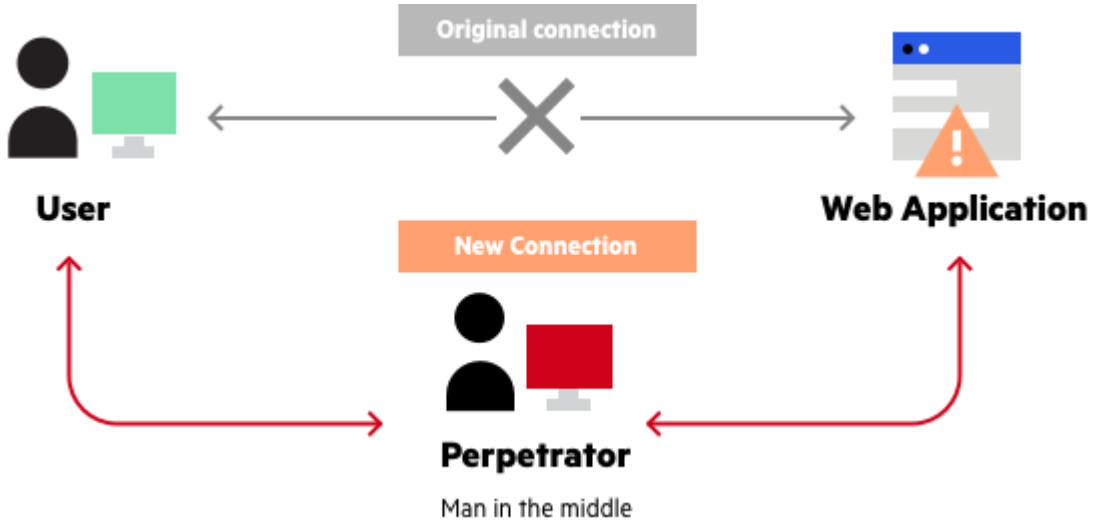
- A denial-of-service (DoS) attack floods a server with traffic, making a website or resource unavailable.

DDoS

- A distributed denial-of-service (DDoS) attack is a DoS attack that uses multiple computers or machines to flood a targeted resource.

MITM Attacks

What is MITM attack. A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.



Phishing Attacks

Phishing is a type of cybersecurity attack during which malicious actors send messages pretending to be a trusted person or entity.

Types of Phishing Attacks

- Spear Phishing
- Whaling
- Smishing
- Vishing

Ransomware

Ransomware is a malware designed to **deny a user or organization access to files on their computer**. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files.

Password Attack

A password attack refers to **any of the various methods used to maliciously authenticate into password-protected accounts**. These attacks are typically facilitated through the use of software that expedites cracking or guessing passwords.

Trojan Horses

A Trojan Horse Virus is **a type of malware that downloads onto a computer disguised as a legitimate program**. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.

Ethical Behavior of Student/Teachers

Digital plagiarism:

Plagiarism is one of the major forms of academic dishonesty which has always existed in education, including higher education. For example, assignments submitted by students may turn out to be copied from fellow students or to be taken over, in part or in whole, from existing published works.

Breaking copyright and software theft:

Throughout the society, it is well known that the illegal copying of copyrighted media (texts, music works, movies and software programs) is widespread. Moreover, many people who engage in such activity do not consider themselves to be doing something that is immoral. This is certainly true for college students.

Improper use of resources:

Students may use their student account to open up a popular website or service that generates loads of traffic, downloads of MP3 files, staff members may use the school's server or computer systems to download or view or store content that is either illegal or against the school policies.

Internet Ethics

Internet ethics means acceptable behavior for using Internet. One should be honest, respect the rights and property of others on the Internet

- Do not use Internet to harm other users
- Do not use Internet to steal others information.
- Do not access files without the permission of the owner.
- Do not download copyrighted software without the author's permission.


MINISTRY OF
HOME AFFAIRS
HELPLINE NUMBER
155260
HAS BEEN
CHANGED TO
1930
If you are a victim of Cyber Crime, Dial 1930 (earlier 155260) &
register your complaint at cybercrime.gov.in

References

- Wikipedia.org
- Tutorialspoint.com
- TechCrunch.com

Thank You ! ! !