Chapter 6
Network Security

Learning Objectives

By the end of this chapter, learner will be able to:

- Name the different kinds of software licensing available
- Differentiate between freeware and open source software
- State how the use of shareware software is different from that of freeware software
- Differentiate between copyright and licensing
- Define cyberethics, cybersafety and cybersecurity
- State the purpose of cookies
- Tabulate the different phases of cyber ethics evolution
- List precautions that can be taken to ensure cyber safety
- Identify the different kinds of threats to cyber security
- State ethical behaviour to be followed as a cyber citizen
- Identify the different categories of cyber crime

INTRODUCTION

The world created by technology is one of machines - computers, computer systems and computer networks. Add to that the human component and one has a world of diverse cultures and social practices that is often referred to as cyberspace.

Cyberspace is a man made world that is constantly evolving. It differs from the static physical world as it has no boundaries, no geographical mass, and of course, no gravity. It is limitless, constantly changing its shape, attributes and characteristics. It exists in a form of bits and bytes; it is an information driven world. Government(s), hardware manufacturers and software application providers act as gatekeepers of cyberspace.

This medium, which is dynamic, infinite and intangible has to be regulated to prevent it from exploding. Regulating cyberspace means regulating both man and the machine. There is ethics, safety and security involved.

Ethics represents personal choice. It's the set of acceptable behaviours in a given culture. It's not just a list of rules but the code of conduct by which a society chooses to live. Safety refers to safe practices and security is the additional tasks carried out to ensure safety.

The first is a moral choice, the second a behavioural code and the third involves active participation.

In cyberspace we have

- **Cyberethics** exploring appropriate and ethical behaviours related to online environments and digital media. It includes plagiarism, bullying, and hacking to name a few.
- **Cybersafety** defining how one operates on-line. It includes rules guiding how to keep personal information safe and limited
- **Cybersecurity** involving tasks undertaken on the computer to keep it secure from people who wish to harm it or use data stored on it unlawfully. This includes installing virus software and firewalls.

Before we study these in greater detail there are certain fundamental terminology and concepts that must be understood.

1. BASIC TERMINOLOGY

1.1 Copyright and License

Copyright is about protecting original expression. Copyright arises as soon as a 'work' is created. A software copyright protects all source code, written text materials, graphic images/ designs, drawings, any linked sound, video files or films.

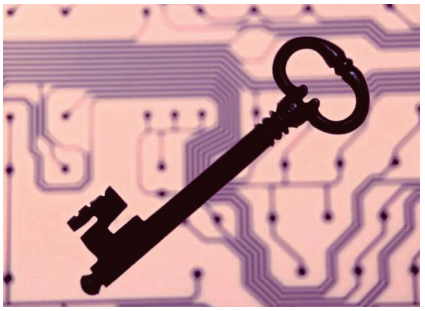
A copyright owner has five exclusive rights:

- Fix or store the information in a tangible form.
- Reproduce the copyrighted material.
- Sell, rent, lease, or otherwise distribute copies of the copyright work to the public.
- Publicly perform and display the copyrighted material.
- Prepare derivative works based on the copyrighted material.

License is the permission granted by the holder of a copyright to another to use an original work. It states under what circumstances and to what extent the original work can be used, changed or distributed. It may include a period of time, a geographical area, renewal provisions, and other limitations. It does not pass on the copyright.

1.2 Software Licensing

A software license is a legal agreement about an application. It is between the software producer and the end-user and is an important part of the legally binding contract between them (or rights owner) and the end-user. This is to ensure recognition of the rights of the owner on his creation. It specifies how the application may be used and defines the rights of both the producer and the user.



1.3 Open Source, Freeware and Shareware

Open-source software (OSS) is computer software with its source code made available. It is very often developed in a public, collaborative manner. A license for open sources software allows the end user to study, change and distribute the software for any purpose.

Some copyrighted software is made available for use, free of charge for an unlimited time. These are called **freeware**. The copyright still remains with the producer / owner for any future development.

Shareware are copyrighted software that can be shared for a limited on a trial basis with the understanding that if the user decides to use it, he will pay for it.

1.4 Types of software licenses

- **Proprietary license** where the copyright stays with the producer and the user is granted the right to use the software
- **GNU General Public Licenses**, which are agreements under which "open source" software is usually licensed. It allows end users to change the source code, but the changed code too, must also be made available under a GNU GPL license.
- **End User License Agreement** (EULA) indicates the terms under which the end-user may use the software.
- **Workstation licenses** are licenses that permit the installation of an application on a single computer. Before installing it on a different machine the software must be removed from the first machine
- **Concurrent use licenses** permit the installation of the software onto multiple machines as long as the number of computers using the software at the same time does not exceed the number of licenses purchased.

- **Site licenses** permit the use of software on any computer at a specified site. Unlimited site licenses allow the installation of the software on any number of computers as long as those computers are located at the specified site.
- **Perpetual licenses** come without an expiry date and allow the software to be used indefinitely
- **Non-perpetual licenses** "lease" the software for use for a specified period of time, usually annually or sometimes bi-annually. Users are required to remove the software from their computer if they cease paying the license fee.
- **License with Maintenance** offer "maintenance" or "software assurance" along with the original license fee.

1.5 Cyber Law

Cyber law is a new branch of law and is growing very fast. It establishes norms of accepted human behaviour in cyberspace. There are three basic building blocks of cyber law.

- Netizens who are the inhabitants of the internet and use it as an extension of their physical world
- Cyberspace which is a 'man made machine world' reshaping itself periodically.
- Technology

Cyber law includes all the cases, written rules and government laws that affect persons and institutions who

- control the entry to cyberspace,
- provide access to cyberspace,
- create the hardware and software which unable people to
  - access cyberspace or
  - Use devices to go 'online' and enter cyberspace.

Laws governing ecommerce, online contracts, copyright, trademark, business software patenting, eTaxation, eGovernance and cyber crimes all fall within the meaning and scope of cyber law.

1.6 Cookies

Cookies allow a visited website to store its own information about a user on the user's computer.

When a user uses a computer to visit a website, the website stores some basic information about the visit on the hard disk of the computer. It records the user's preferences while using the site. This stored information is called a 'cookie'.

1.7 Hackers and Crackers

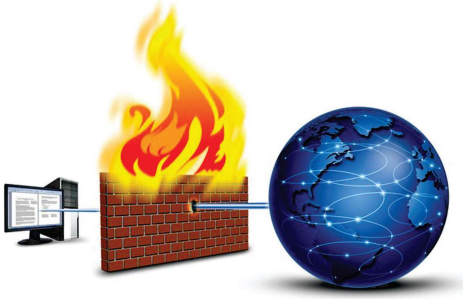
Hackers are people with computer programming skills who use their knowledge to gain unauthorized access to data in a system or computer.

Crackers modify or disable features of a software application. They usually mean to harm the software, the hardware using this software or the end user of the software.

Both hackers and crackers can also work on the ethical side when they use their skills to prevent cyber crime and help the law keepers.

1.8 Firewall

A firewall is a program or hardware device that filters the information coming through an internet connection to a network or computer system. If incoming information does not pass the rules stored in the firewall, it is not allowed through.



1.9 Cyber Ethics

The explosion of social networking and the common practice of sharing and posting of information online have changed the way people communicate. Users must understand their responsibilities for conducting themselves online. An important component of that is Cyber Ethics. Cyber Ethics refers to the code of responsible behaviour on the Internet. Basic Cyber ethics must be followed to be good cyber citizens.

Cyberethics began in some form in the 1940s. It examines the impact of not only the internet or computing machines but also private computer networks and interconnected communication technologies.

The evolution of cyber ethics can be categorized in four distinct phases.

Phase	Time Period	Technological features	Associated issues
I	1950s - 1960s	• Stand alone machines (Large mainframe computers)	• Artificial intelligence • Database privacy
II	1970s - 1980s	• Minicomputers • PCs • Privately owned computer networks	• Problems of Phase I • Intellectual property • Software piracy • Computer crime • Privacy and exchange of data
III	1990s – Present	• Internet • The World Wide Web (www)	• Problems of Phase I and II • Concerns about free speech • Anonymity • Legal jurisdiction • Virtual communities
IV	Present - Near Future	• Convergence of information and communication technologies • Nano technology research • Genetic and genomic research	• Problems of Phase I, II and III • Concerns about artificial electronic agents (bots) with decision making capabilities • Biochip implants

Cyber ethics must be practiced at every level of computer use—from the novice user to an information technology professional whose job requires significant use of online resources. Those who use the internet must be follow ethical practices in every aspect of its use.

Anyone can communicate at anytime, with anyone, anywhere over the internet today. This can have negative consequences. Anonymous posting to blogs, websites, and social media can encourage bad behaviour as it does not identify the person who commits the action.

With the widespread availability of mobile phones and internet access, bullying and harassment can be conducted through cyberspace. Developments in electronic media offer new platform for bullies and allow cyber bullying. Cyber bullying

uses internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, web pages or SMS (text messaging) - with the intention of harming another person. The actions can range from cruel or embarrassing rumours to threats, harassment, or stalking. The effects can be far-reaching and long lasting.

The same rules of right and wrong taught to a child while growing up needs to be applied to cyber space! Do not do something in cyber space that you would consider wrong or illegal in everyday life.

- Do not use rude or offensive language.
- Do not lie about people, send embarrassing pictures of them, or anything else to try to hurt them (bullying).
- Do not use someone else's password or break into his computer.
- Do not copy information from the Internet and claim it as yours (plagiarism).
- Obey copyright restrictions when downloading material.
- Do not try to make someone else's computer unusable.

1.10 Cyber Safety

Identity theft is a growing problem and a very troubling one. The concept is rather simple, though the process can be complex, and the consequences for the victim can be quite severe. The idea is simply for one person to take on the identity of another. This is usually attempted to make purchases; but identity theft can be done for other reasons, such as obtaining credit cards in the victim's name, or even a driver's licenses. If the person responsible for the theft obtains a credit card in someone else's name, then he can purchase products and the victim of this fraud is left with debts she was not aware of and did not authorize.

One of the more common ways to accomplish identity theft is via a technique called **phishing**, which is the process of trying to tempt the target to provide personal information which can be used to perform illegal actions.

Another horrifying safety threat is stalking which involves harassing or threatening behaviour that an individual engages in repeatedly. It could mean following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Such behaviour should be treated seriously.

Cyber-safety addresses the ability to act in a safe and responsible manner on the Internet and other connected environments. These behaviours protect personal information and

reputation. They include safe practices to minimize danger from behaviour-based rather than hardware/software-based problems.

In following cyber safety guidelines a user will recognize online risks, make informed decisions, and take appropriate actions to protect himself while using technology, technology systems, digital media and information technology. He would adhere to privacy and safety guidelines, policies, and procedures.

Here are some cyber safety guidelines to follow.

- Set secure passwords and don't share them with anyone. Avoid using common words, phrases, or personal information and update regularly.
- Restrict access and make personal information secure to prevent identity theft.
- Be suspicious of unsolicited contact from individuals seeking internal organizational data or personal information. Verify a request's authenticity by contacting the requesting entity or company directly.
- Immediately report any suspect data or security breaches to your supervisor and/or authorities.
- Limit the amount of personal information you post. Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your friend posts information about you, make sure the information is something that you are comfortable sharing with strangers.
- Be wary of strangers and cautious of potentially misleading or false information.
- Take advantage of privacy and security settings. Use site settings to limit the information you share with the general public online.
- Be suspicious of unknown links or requests sent through email or text message. Do not click on unknown links or answer strange questions sent to your mobile device, regardless of who the sender appears to be.
- Download only trusted applications from reputable sources or marketplaces.

1.11. Cyber Security

The media gives a lot of attention to dramatic virus attacks, hackers, and other interesting Internet phenomena. In spite of daily horror stories, however, many people lack an adequate understanding about the reality of these threats.

External threat to any system is not just hackers or crackers, but also malware and denial of service attacks. Malware includes viruses, worms, Trojan horses, and logic bombs. And there is the issue of internal problems due to misbehaviour or simple ignorance.

2. MOST ATTACKS CAN BE CATEGORIZED AS ONE OF SIX BROAD CLASSES

Malware, software that has a mischievous purpose such as virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to a system. Malware is discussed in detail later in the lesson.

Security breaches that attempt to gain unauthorized access to a system including cracking of passwords, changing privileges, breaking into a server….. in other words, hacking a computer or a computer network.

Denial of service (DoS) attacks that are designed to prevent legitimate access to a system.

Web attacks that attempts to breach a website. Two of the most common such attacks are SQL injection and cross-site scripting.

Session hijacking, where an attacker attempts to take over a session.

DNS poisoning, which seeks to compromise a DNS server so that users can be redirected to unsafe websites.

Malware

Malware is used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software. Let us take a look at some of the important malwares available today.

Viruses: A computer virus is a program that replicates itself. A computer virus attaches itself to a program or file to help it spread from one computer to another. Almost all viruses are attached to an executable file, which means the virus may exist on a computer but it actually cannot infect the computer unless one runs or opens the malicious program. It is important to note that a virus cannot be spread without a human action, (such as running an infected program) to keep it going.

Generally, a virus will also have some other unpleasant function, but the self-replication and rapid spread are the distinguishing features of a virus. Often this growth, in and of itself, can be a problem for an infected network. The infamous 'I Love You' virus slowed down many networks just by the volume of emails it generated.

Worms: A worm is similar to a virus and is considered to be a sub-class of a virus. It spreads from computer to computer, as it has the capability to travel without any human action. A worm takes advantage of file or information transport features on a system, which is what allows it to travel unaided. Worms cause harm to the infected network, whereas viruses corrupt or modify files on a targeted computer. In recent worm attacks such as the much-talked-about Blaster Worm, the worm has been designed to tunnel into a system and allow malicious users to control the computer remotely.

Adware: Adware refers to computer software that is provided usually for free but contains advertisements. It automatically renders advertisements in order to generate revenue for its author.

Trojan horses: A Trojan horse is a program that looks straightforward and safe but actually has a malicious purpose. At first glance it will appear to be useful software but will actually do damage once installed or run on a computer. It is often used to deliver a virus into the system. One of the earliest and most widely known was Back Orifice.

Spyware: Spyware is simply software that literally spies on what is being done on a computer. Spyware can be as simple as a cookie used by a website to record a few brief facts about a visit to that website, or spyware could be of a more dangerous type such as a key logger, a program that records every keystroke one makes on a keyboard.

The DOs and DONTs of network security

- Pay close attention to website URLs. Pay attention to the URLs of websites you visit.
- Keep operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies.
- Turn off the option to automatically download attachments from your emails
- Save and scan any attachments before opening them. If you have to open an attachment before you can verify the source, take the following steps:
  - Be sure your anti-virus software is up to date.
  - Save the file to your computer or a disk.
  - Run an anti-virus scan using your computer's software.

3. CYBER CRIMES

Now that we are familiar with a number of network security concepts and vocabulary let us take a look at where all this is leading. With enhanced technology, cyber crimes are the norm today.

Cyber crime may be defined as any illegal act that involves a computer, computer system or computer network. It is any illegal act for which knowledge of computer technology is essential to execute, investigate, or implement.

3.1 Types of Cyber Crimes

Cyber crime can be categorized as given here.

- General Intrusions
  - Hacking, spyware, phishing, pharming,
  - Sending computer viruses & worms to invade computers
  - Causing denial of service attacks
  - Creating bots, Trojan horses, zombie machines
- Nuisances (usually non-violent activities)
  - Sending spam
  - Changing web page text and images
  - Redirecting websites
- Personal Identity Theft (using someone else's name or credit)
  - Phishing for private information, passwords, code numbers
  - Making unauthorized purchases with stolen credit cards or ID
  - Destroying personal reputation
  - Damaging personal credit ratings
- Theft of Intellectual Property (stealing ideas or creations of others)
  - Downloading copyrighted music & videos
  - Plagiarism, cheating
  - Software piracy
- Physical or Mental Damage
  - Cyberbullying, harassment
  - Cyberstalking
  - Sexual exploitation of minors, child pornography

- Terrorism
  - Stealing military and private industry secrets - espionage
  - Brainwashing and recruiting new followers
  - Building terrorist communications network

Some of these we have already talked about in the lesson. You could find out information about the others from other sources. This is just an introduction to get you going.

General Intrusions

Case 1: **Sending Computer Virus/Worm to invade computers**

The ILOVEYOU virus comes in an e-mail note with "I LOVE YOU" in the subject line and contains an attachment that, when opened, results in the message being re-sent to everyone in the recipient's Microsoft Outlook address book and, perhaps more seriously, the loss of every JPEG, MP3, and certain other files on the recipient's hard disk. Because Microsoft Outlook is widely installed as the e-mail handler in corporate networks, the ILOVEYOU virus can spread rapidly from user to user within a corporation. On May 4, 2000, the virus spread so quickly that e-mail had to be shut down in a number of major enterprises such as the Ford Motor Company. The virus reached an estimated 45 million users in a single day.

The attachment in the ILOVEYOU virus is a VBScript program that, when opened (for example, by double-clicking on it with your mouse), finds the recipient's Outlook address book and re-sends the note to everyone in it. It then overwrites (and thus destroys) all files of the following file types: JPEG, MP3, VPOS, JS, JSE, CSS, WSH, SCT and HTA. Users who don't have a backup copy will have lost these files. (In March 1999, a virus named Melissa virus also replicated itself by using Outlook address books, but was less harmful in destroying user files.) The ILOVEYOU virus also resets the recipient's Internet Explorer start page in a way that may cause further trouble, resets certain Windows registry settings, and also acts to spread itself through Internet Relay Chat (Internet Relay Chat).

The Creators Reomel Ramores and Onel de Guzman created this deadly virus on 5 May 2000 but were lucky to escape prosecution due to lack of rules for arresting people for writing malicious code in Philippines ! The Damage-- 50 million infections reported within 10 days.

Case 2: **Malware/Trojans**

A Trojan takes its name from the term 'Trojan Horse'. It is a type of computer virus that can be installed on your computer without you realising.

One variation of a Trojan installs a 'keystroke logger' on your computer. This records the words and numbers you type when you use your computer keyboard. If you login to your online bank account, the keystroke logger will record your login information.

More sophisticated Trojans insert a pop-up page in front of your genuine online banking page, and then try to trick you into making a payment to someone else's account.

Other types of malware are able to insert extra fields, not normally found on your online banking website.

It is suggested that you should use **virtual keyboard** while doing net banking. Virtual Keyboard is an online application to enter password with the help of a mouse.The Virtual Keyboard is designed to protect your password from malicious "Spyware" and "Trojan Programs". Use of Virtual keyboard will reduce the risk of password theft.

Case 3: **Stealing internet user name and password**

Vivan and Arpit of a reputed Computer training Institute sent emails to different banks, offices purportedly from reputed senders like Microsoft Support Team, VSNL helpdesk etc with the subject line 'double your internet speed'.

Actually they sent some sort of trojan sniffer in the guise of these executable files.

When recipients ran the file, a software called Dialup Security became resident in the computer memory and started working whenever the user booted the computer. When the user accessed the internet, the Trojan captured the username and password fields from the dialup screen and sent a mail to the culprits in encrypted form.

Case 4: **Email Fraud**

Diploma Scam

Quick degree scams - "Get your degree in 30 days!" "No studying required", "Turn your experience into a degree". They say they are accredited and the degree is legal and meaningful. That's part of the scam.

The existence of unaccredited, substandard, and/or fraudulent post-secondary education (college, university, graduate schools) providers is a global phenomenon, as is the existence of unrecognized and/or fraudulent accreditors. The credits and degrees awarded by these unaccredited or sham diploma mills are not going to be recognized by legitimately accredited institutions, official professional licensing authorities, recognition authorities or reputable employers.

And when the scam is exposed that you purchased your degree; you'll be out on the street and no one will hire you. You may make the cover of a newspaper, exposed as the worthless hack you are for attempting to buy your degree. You may make a list of people who have purchased scam degrees, that we're working on right now.

Personal Identity theft

Spamming, Redirecting websites & Phishing

Case 5: **Phishing**

One financial Institute registered a crime stating that some persons ("perpetrators") have perpetrated certain acts through misleading emails ostensibly emanating from a National Bank's email ID. Such acts have been perpetrated with an intent to defraud the Customers.

The Investigation was carried out with help of those emails received by the customers of that financial Institute and arrested the accused, the place of offence at Vijaywada was searched for the evidence. There one Lap Top and Mobile Phone was seized which was used for the commission of the crime

The arrested accused had used open source code email application software for sending spam emails. He has down loaded the same software from net and then used it as it is.

He used only VSNL emails to spam the email to customers of financial Institute because VSNL email service provider do not have spam box to block the unsolicited emails.

After spamming emails to financial Institute customers he got the response from around 120 customers of which 80 are genuine and others are not correct because it do not have debit card details as required for e-banking.

The financial Institute customers those who have received his email felt that the email was originated from the financial Institute bank. When they filled the confidential information and submitted that time said information was directed to accused. This was possible because the dynamic link was given in the first page (Home page) of the fake web site. The dynamic link means when people click on the link provided in spamming email that time only the link will be activated. The dynamic link was coded by handling the Internet Explorer onclick() event and the information of the form will be submitted to the web server (Where the fake web site is hosted). Then server will send he data to configured email address and in this case email configured was to the accused email . So on submission of the confidential information the information was directed to email ID accused email .The

all the information after fishing (user name, password, Transaction password, Debit card Number and PIN, mothers maiden name) which he had received through Wi-Fi internet connectivity of Reliance.com which was available on his Acer Lap Top.

This crime has been registered u/s U/Sec. 66 of IT Act, sec 419, 420, 465, 468, 471 of I.P.C r/w Sections 51, 63 and 65 of Copyright Act, 1957 which attract the punishment of 3 years imprisonment and fine up to 2 lacs rupees which accused never thought of.

How does phishing happen?

- Phishers sets up a replica page of a known financial institution or a popular shopping website
- Bulk e-mails are sent to users asking for their personal data like account details, passwords etc
- When the user clicks on the link, the replica of the website will open. Or while the user is online, a form will populate through an "in-session pop-up"
- On updation, the data goes to phishers. Post which the user is redirected to the genuine website

Phishers have refined their technology to launch sophisticated attacks and use advanced social engineering techniques to dupe online banking users.

Case 6: **Hacking**

Mumbai police have arrested a hacker by name Kalpesh (name change) for hacking into a financial website. Although the hacker couldn't break into the main server of the financial institution, which was well secured by the financial institution. The accused person could make some addition to the home page of the financial website and has added a string of text to the news module of the home page of the website. Police were able to crack the case by following the trace left by the hacker on the web server of the financial institution. The financial institution has maintained a separate server for financial online transactions, for which utmost security has been taken by the financial institution. The website was hosted on a different server which comparatively had lesser security.

The hacker Kalpesh (name changed) is a 10th Pass youngster of 23 years old. He has done computer courses like CCNA, MCSE etc. But he is a computer addict. He sits before the computer for almost 16 to 20 times each day. He has mostly used the readymade hacking tools, to hack into any website. He goes to a particular website on the web, which facilitates him to see the entire directory structure of that website. Then using various techniques, such as obtaining a password file, he gets into the administrator's shoes and hacks the website.

A case has been registered against the hacker under section 67 of Information Technology Act – 2000 and under various sections of Indian Penal Code.

Cyberstalking, cyberbullying, Sexual exploitation

Case 7: Cyber bullying

In April 2001 a person from New Delhi complained to the crime branch regarding the website. Amazing.com, he claimed, carried vulgar remarks about his daughter and a few of her classmates. During the inquiry, print-outs of the site were taken and proceedings initiated.

After investigation a student of grade XI and classmate of the girl was arrested. The juvenile board in Nov 2003 refused to discharge the boy accused of creating a website with vulgar remarks about his classmate.

Case 8: Cyberstalking

There are a couple of reported cases, which speak of the position of the cyber stalking in India. The recent being the case of A(name) who was recently arrested by the New Delhi Police. He was talking an Indian lady, B(name) by illegally chatting on the Web site MIRC using her name. He used obscene and obnoxious language, and distributed her residence telephone number, inviting people to chat with her on the phone. As a result of which, B kept getting obscene calls from everywhere, and people promptly talked dirty with her. In a state of shock, she called the Delhi police and reported the matter. For once, the police department did not waste time swinging into action, traced the culprit and slammed a case under Section 509 of the Indian Penal Code for outraging the modesty of B (Indian child, 2005).

Both kind of Stalkers "Online & Offline" – have desire to control the victims life. Majority of the stalkers are the dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their secret desires. Most of the stalkers are men and victim female.

How do they Operate

a. Collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such

as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

b. The stalker may post this information on any website related to relationship, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have services. Stalker even uses very filthy and obscene language to invite the interested persons.

c. People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for relationships.

d. Some stalkers subscribe the e-mail account of the victim to innumerable pornographic sites, because of which victim starts receiving such kind of unsolicited e-mails.

e. Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.

f. In online stalking the stalker can make third party to harass the victim.

g. Follow their victim from board to board. They "hangout" on the same BB's as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed. Many times they will "flame" their victim (becoming argumentative, insulting) to get their attention.

h. Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.

i. Contact victim via telephone. If the stalker is able to access the victims telephon, he will many times make calls to the victim to threaten, harass, or intimidate them.

j. Track the victim to his/her home.

Case 9: **Cyber Pornography**

A student of a reputed public school was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.

Cyber pornography case the first case of this kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the IT act, 2000.

Case 10: **Social Networking**

A 14-year-old girl received a Facebook friend request from an older man posing as a boy of her age. She accepted it out of curiosity.

The girl was quickly smitten by the man's smooth online flattery. She didn't realise that he was one of the growing number of sexual predators who had found a new way to exploit the increasing obsession with social media.

They exchanged phone numbers, and his attention increased with rapid-fire texts. He convinced her to meet in a mall, and she found him just as charming in person.

They agreed to meet again. After telling her mom she was going to visit a sick girlfriend, she climbed into the man's minivan near her home.

The man, a 24-year-old drove her an hour to a town .There, he locked her in a small room inside a house with at least five other girls aged 14 to 17.She came to know that she was kidnapped. She somehow managed to escape ,but everyone does not get a chance.

Ways to protect yourself on social networking sites:

Limit who can see what you post. If you don't want random users to see your contact information, you can limit the publication of that data. Just change your settings. You can also block users from having any contact with you should the need arise.

One simple and quick setting (on Facebook) you can change to increase privacy is to restrict the viewing of your profile only to users at your own college or to only your "friend" list. Most social networking sites offer similar ways to restrict access to personal information, but in all cases, the principle is the same: don't advertise to the world what you're doing or where you live.

But don't forget that even if you limit who can see what you post, there are ways others can get around it to view your profile anyway.

Limit what you post. Don't share things that would make you vulnerable to unwanted contact (such as sharing your email address, physical address, or phone number) or to stalking (such as information about your schedule or routine).

Also, if your friends or connections post such information about you, make sure the combined information on their pages is not more than you would be comfortable with strangers knowing.

Finally, it's important to recognize that once you publish something online, it is available to other people and to search engines. *You can't retract it.*

Even if you go back and remove the information from a site, it's always possible that someone has already seen it. And they may have saved a copy.

In addition, some search engines "cache" copies of Web pages so that they open faster; these cached copies may be available a long time after a Web page has been deleted or altered. Some Web browsers, also, maintain a cache of the Web pages a user has visited, so the original version of your posting may be stored in someone else's machine.

The bottom line? Once something is out there, there's no guarantee you can take it back.

Tracking Cyber Crimes

Case Study: **Admission fraud**

A girl Anita (name changed) came to cyber cell with a complaint. As per the complaint she registered her self with an admission counsellor for admission in a foreign university. After registration she received a call from a lady named Sameera (name changed)who was working as counsellor with a reputed admission consultant firm in United Kingdom, for the interview. Anita was very happy to hear that. Her interview was taken over telephone and she was given provisional admission and letter was sent through email. Another day Sameera called Anita and told her that she has been awarded scholarship and she has to start a current account in either AXIS bank or HDFC bank with current account limit upto Rs. 25,000/-. She agreed and did the same. After opening the account Anita supplied the relevant details of account to Sameera, as she was told that the university will deposit Rs. 1.90 lakh in her account and she will have to withdraw Rs. One Lakh and will have to deposit the same in six different accounts and rest amount will be her scholarship money. It happened the same way as told by Sameera. Anita checked her account and it was showing credit of Rs.1.90 Lakh.

Next day Anita approached the bank to withdraw money and deposit the same in to six different accounts but due to some technical reasons see could not withdraw the money from her HDFC account having credit of Rs 1.90 lakh. Anita was in belief that she has already received the amount hence deposited her own money in six different accounts which were from Uttrakhand and Delhi. Next day Anita went again to the bank to withdraw money but she was shocked to hear that her account has been blocked by Lucknow police and an FIR has already been lodged at Lucknow police station against her and she is the prime suspect. On receiving a complaint Cyber cell started enquiry from the emails received by Anita. The full header analysis revealed ip address and the same was sent to mobile operator which ended to a mobile number. The name and address attached to the mobile number were found to be false which were supposed to be from Mumbai. Cyber cell collected the login logs of the internet banking account of Mr Manish (name changed) and found that money was hacked and transferred from Nigerian IP.

Subsequently Cyber cell registered a FIR under section 66 IT act , 420/34 IPC

Name and address of the mobile used by Sameera were in the name of Nigerian Franklin (name changed). The address was not reachable as he shifted to new address. After that cyber cell started analysing the logs of Sameera and identified the numbers to whom call was made. Finally cyber cell had five numbers to be analyzed. After months of analysis one suspect was traced. Cyber cell had the address of a suspect, the house was raided by cyber cell at Delhi and seized 6 mobiles and a laptop but accused could not be caught. LOC was issued against suspect. During investigations the culprits were identified to be O. Addeda (name changed) and her lady co-partner. Mobiles and laptops involved in the fraud were recovered from Addeda's house but he escaped. After analysis of Addeda mobile cyber cell found the person named EMMA to be the prime suspect providing bank details to him. Documents seized also show his relation with him. Analysis of CDR revealed that EMMA (name changed) is superior in hierarchy of internet job fraud.

Cybercell has arrested EMMA and his wife from their home. Several bank details, ATM/ DEBIT cards were recovered from him. At present EMMA is in CENTRAL JAIL and is facing trial. His wife co-accused in the crime has been given bail due to last stage of pregnancy. Court has issued permanent arrest warrants against the accused who are absconding. Cyber cell is trying to identify the properties owned by the suspects so that proceeds of the frauds can be recovered from them.

Summary

Cyberspace is a man made world that is constantly evolving. It differs from the static physical world as it has no boundaries, no geographical mass, and of course, no gravity.

1. Cyber ethics exploring appropriate and ethical behaviours related to online environments and digital media. It includes plagiarism, bullying, and hacking to name a few.
2. Cyber safety defining how one operates on-line. It includes rules guiding how to keep personal information safe and limited.
3. Cyber security involving tasks undertaken on the computer to keep it secure from people who wish to harm it or use data stored on it unlawfully. This includes installing virus software and firewalls.
4. A software copyright protects all source code, written text materials, graphic images/ designs, drawings, any linked sound, video files or films.

License is the permission granted by the holder of a copyright to another to use an original work. It states under what circumstances and to what extent the original work can be used, changed or distributed.

1. **Open-source** software (OSS) is computer software with its source code made available. It is very often developed in a public, collaborative manner. A license for open sources software allows the end user to study, change and distribute the software for any purpose.
2. Some copyrighted software is made available for use, free of charge for an unlimited time. These are called **freeware**. The copyright still remains with the producer / owner for any future development.
3. **Shareware** are copyrighted software that can be shared for a limited on a trial basis with the understanding that if the user decides to use it, he will pay for it.
4. Cyber law is a new branch of law and is growing very fast. It establishes norms of accepted human behaviour in cyberspace.
5. Cookies allow a visited website to store its own information about a user on the user's computer.
6. A firewall is a program or hardware device that filters the information coming through an internet connection to a network or computer system.

Hackers are people with computer programming skills who use their knowledge to gain unauthorized access to data in a system or computer.

Crackers modify or disable features of a software application. They usually mean to harm the software, the hardware using this software or the end user of the software.

EXERCISE

A. Multiple choice questions

1. Which of the following is not an external threat to a computer or a computer network
   (a) Ignorance (b) Trojan horses
   (c) Adware (d) Crackers

2. When a person is harrassed repeatedly by being followed, called or be written to he / she is a target of
   (a) Bullying (b) Identity theft
   (c) Stalking (d) Phishing

3. With genetic and genomic research which of the following issues is of specific concern
   (a) Anonymity (b) Intellectual property
   (c) Software piracy (d) Concerns about biochip implants

4. Which of the following is a class of computer threat
   (a) Phishing (b) DoS attacks
   (c) Soliciting (d) Stalking

5. A lincense allows a user to use copyrighted material.
   (a) True (b) False

6. It is a program or hardware device that filters the information coming through an internet connection to a network or computer system.
   (a) Anti virus (b) Firewall
   (c) Cookies (d) Cyber safety

7. It allow a visited website to store its own information about a user on the user's computer.
   (a) Spam (b) Malware
   (c) Cookies (d) Adware

8. It is stealing ideas or creations of others.
   (a) Plagiarism (b) Piracy
   (c) Intellectual Property Rights (d) All of the above

9. Hacking a computer is always illegal and punishable by law.
   (a) True (b) False

10. Exploring appropriate and ethical behaviours related to online environments and digital media.
    (a) Cyber ethics (b) Cyber safety
    (c) Cyber security (d) Cyber law

11. A lincense allows a user to use copyrighted material.
    (a) In some situations this statement is correct
    (b) This statement is not true at all.
    (c) In is not necessry to use license.
    (d) All the above statements are not applicable.

B. Answer the following questions:

1. Differentiate between a workstation license and a site license.
2. Write a short note on your understanding of 'cracking' a software.
3. What are the categories of Cyber crime. Explain them.
4. Define the following terms:
   (a) Spyware (b) Malware
   (c) Virus (d) Worms
5. Read about ethical hacking and write a short note on your understanding of the topic.
6. Why cyber security should be taken care by the user while working on internet?
7. Discuss all the point which should be kept in mind while working on computers.
8. What is Deniel of Service attack? How it affects the systems performance?
9. What is the difference between Shareware and Freeware softwares?
10. Mention the list of the licenses used by the users.
11. What do you mean by open source softwares? How are they different from properitary softwares?
12. In groups of 4-5 discuss how software cookies can be 'helpful' to both the user of the computer and the websites that created them. Document your understanding. It could be a poster, a brochure, a poem or a skit.
13. What all do you ususally do while you are connected to the net? Make a list and then plan all the security measures that you could take to safeguard yourself. Share this list eith at least two of your peers and compare it to their lists.

C. Categorize the following under ethical / safety / security precaution

1. Do not share your password
2. Do not use foul language.
3. Immediately report any suspect data or security breaches to your supervisor and/or authorities.
4. Install firewalls and antivirus softwares

5. Do not copy information from the Internet and claim it as yours (plagiarism).
6. Be wary of strangers and cautious of potentially misleading or false information.
7. Manage your computer settings to allow only data that comes from a known or safe place
8. Do not download copyrighted materials.
9. Download only trusted applications from reputable sources or marketplaces
10. Pay attention to the URLs of websites you visit
11. Do not use someone else's password or break into his computer.
12. Restrict access and make personal information secure to prevent identity theft.

D. State whether the following statements are true or fal

1. Hacking a computer is always illegal and punishable by law.
2. A lincense allows a user to use copyrighted material.
3. Software can only be licensed for a specific period of time.
4. A firewall is a virtual 'wall' that protects data on computers and computer networks.
5. Cyber law oversees only crimes that are committed by computers.
6. Crackers use physical tools to break into a computer and steal data.
7. Read about ethical hacking and write a short note on your understanding of the topic.
8. In groups of 4-5 discuss how software cookies can be 'helpful' to both the user of the computer and the websites that created them. Document your understanding. It could be a poster, a brochure, a poem or a skit.
9. What all do you ususally do while you are connected to the net? Make a list and then plan all the security measures that you could take to safeguard yourself. Share this list eith at least two of your peers and compare it to their lists.