Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

III B.SC PSYCHOLOGY

21CPS5C-CYBER PSYCHOLOGY

INTRODUCTION TO CYBER PSYCHOLOGY

Introduction: Definition - Origin of Cybernetics - Origin of Artificial Intelligence in Cybernetics-Cyber Behaviour: Educational, Employment, Health. Cyber Space: Basic Psychological Qualities of Cyber Space - On-Line Identity - On-Line Relationship-Personality Types in Cyber Space - Computer and Cyber Space Addiction

Definition

Cyber psychology is an emerging field of study focusing on information communication technology (ICT) and its impact on human behaviour at the individual and societal level.

-Dr Andrew J. Campbell

Origin of cybernetics

- Cybernetics began properly with the publication, in 1948, of a book by Norbert Wiener entitled “Cybernetics or Control and Communication in the Animal and the Machine”. The word cybernetics had been chosen by Wiener, in agreement with other colleagues, from the Ancient Greek kubernetike, or the art of steering.
- Another initiator, almost as important as Wiener, is Warren S. McCulloch who published, in 1943, in collaboration with N. Pitts, an article on logics and the nervous system.
- Wiener’s preference was due to Leibniz’s interest in the construction of a calculating machine, and his attempt to build up a general calculus of logics (logical theory).
- J. von Neumann had contact with Wiener and McCulloch, mainly in a group sponsored by the Macy Foundation called the Teleological Society, or informally the “Cybernetic Club”., philosophers and physicians
- Later with the help of two more mathematicians, philosophers and physicians a lot of conceptions has been added to the domain of cybernetics

Origins of AI (artificial intelligence) in cybernetics:

- The seed of modern Al was planted by classical philosophers who wanted to describe human thinking as a mechanical manipulation.
- The Al research founded at Dartmouth college in summer 1956 and "John McCarthy is regarded as father of Al".

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

- The project faced difficulty in 1973 in response to criticism of James Light hill and on-going pressure from government and stopped funding on directed research into Al.
- Investment and interest in Al boomed in first decade of 21st century.
- Study of cybernetics and neural network help in constructing an electric brain.
- Alan Turing provide a Turing test in which it make sure that machine is thinking.

Cyber behaviour

Cyber behaviour results from the use of many different devices we have become reliant on. We are also most likely to be unaware of how these devices affect our social and cognition interaction with others

Education

Pre-cyber generation	Post-cyber generation
High level commuting • Library resources • Reduced media • Longer information processing (Deep learning) • Longer production time • Isolation study (normal	Reduced commuting • internet + Library • Increased media • Shorter information processing (surface learning) • Shorter production time • Supportive study online

Employment

Pre-cyber generation	Post-cyber generation
Reliant on Newspapers / word-of-mouth / employment centres. • Lengthy interview processes (to deduce skills and personal qualifications). • Hidden employment opportunities. • In some cases, less comprehensive employee screening. • Fewer interview preparation resources communicated.	Multitude of ICT + Pre-Cyber resources • Online employment screening + e-services • Shorter interview processes (More individually focused). • Employment choices are abundant (but are they communicated well?) • Increased employee screening (is it effective?) • More resources for C.V. and Interview Preparation

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Health

Pre-cyber generation	Post-cyber generation
Personal Health informed by Doctor/Allied Health. • Limited Drug information. • Self-treatment information/ options limited available, as is self-medication (ethical?) • Health costs in some cases were higher. • Not empowered about own health.	Personal Health is becoming pro active • Drug information is more accessible (but reliable?) • Self-treatment is readily • Health costs can be more closely managed, especially with prescription choices. • Highest level of health empowerment measured in modern history! (W.H.O.)

CYBER SPACE

Cyberspace is the electronic medium of computer networks, in which online communication takes place. It is readily identified with the interconnected information technology required to achieve the wide range of system capabilities associated with the transport of communication and control products and services.

BASIC PSYCHOLOGICAL QUALITY OF CYBER SPACE

Reduced Sensations

Multimedia gaming and social environments, audio-video conferencing, podcasting, and internet-phoning surely are signs of the very sensory sophisticated environments to come. However, the sensory experience of encountering others in cyberspace - seeing, hearing, and COMBINING seeing and hearing - is still limited. For the most part people communicate through typed language. Even when audio-video technology becomes efficient and easy to use, the quality of physical and tactile interactions (example, handshakes, pats on the back, dancing, hugs, kisses, or just walking together) will be very limited or non-existent, at least in the near future. The limited sensory experiences of cyberspace have some significant disadvantages - as well as some unique advantages - as compared to in-person encounters.

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Texting

Despite the reduced sensory quality of text communication, it should not be underestimated as a powerful form of self-expression and interpersonal relating. E-mail, chat, instant messaging, SMS, and blogs continue to be the most common forms of social interaction for reasons beyond their ease of use and low cost compared to multimedia tools. Drawing on different cognitive abilities than talking and listening, typing one's thoughts and reading those of another is a unique way to present one's identity,

Identity Flexibility

The lack of face-to-face cues has a curious impact on how people present their identity in cyberspace. Communicating only with typed text, you have the option of being yourself, expressing only parts of your identity, assuming imaginative identities, or remaining completely anonymous - in some cases, being almost invisible, as with the "lurker." In many environments, you can give yourself any name you wish. The multimedia worlds also offer the opportunity to express yourself through the visual costumes known as "avatars."

Altered Perceptions

Sitting quietly and staring at the computer monitor can become an altered state of consciousness. While doing e-mail or instant messaging, some people experience a blending of their mind with that of the other person. In the imaginary multimedia worlds - where people might shape-shift, speak via ESP, walk through walls, spontaneously generate objects out of thin air, or possess all sorts of imaginary powers - the experience becomes surrealistic. It mimics a state of consciousness that resembles dreams. These altered and dream-like states of consciousness in cyberspace may account for why it is so attractive for some people. It might help explain some forms of computer and cyberspace addiction.

Equalized Status

Everyone on the internet has an equal opportunity to voice him or herself. Everyone - regardless of status, wealth, race, gender, etc. - starts off on a level playing field. Some people call this the "net democracy." Although one's status in the outside world ultimately will have some impact on one's life in cyberspace, there is some truth to this net democracy ideal. What determines your influence on others is your skill in communicating (including writing skills), your persistence, the quality of your ideas, and your technical know-how.

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Transcended Space

Geographical distance makes little difference in who can communicate with whom. The irrelevance of geography has important implications for people with unique interests or needs. In their outside life, they may not be able to find anyone near them who shares that unique interest or need. But in cyberspace, birds of a feather - even those with highly unusual feathers - easily can flock together. For support groups devoted to helping people with their problems, that can be a very beneficial feature of cyberspace. For people with antisocial motivations, that's a very negative feature of cyberspace.

Temporal Flexibility

"Synchronous communication" involves people sitting at their computer at the same time (i.e., in "real time") communicating with each other via the internet. Chat rooms and instant messaging are good examples. On the other hand, e-mail and newsgroups involve "asynchronous communication" that does not require people to interact with each other in the moment. In both asynchronous and synchronous communication (with the exception of video conferencing and internet phoning), there is a stretching of time. Cyberspace creates a unique temporal space where the ongoing, interactive time together stretches out. This provides a convenient "zone for reflection." Compared to face-to-face encounters,

Social Multiplicity

With relative ease a person can contact people from all walks of life and communicate with hundreds, perhaps thousands of people. While "multitasking" one can juggle many relationships in a short period of time - or even AT the same time, as in chat and instant messaging, without the other people necessarily being aware of one's juggling act. By posting a message within a blog, discussion board, or social network - which are read by countless numbers of users. Using a search engine, they can scan through millions of pages in order to zoom their attention onto particular people and groups.

Recordability

Most online activities, including e-mail correspondence and chat sessions, can be recorded and saved to a computer file. Unlike real world interactions, the user in cyberspace can keep a permanent record of what was said, to whom, and when. Because these interactions are purely document-based. Although the ability to record has many advantages, there is a downside. Because people know that everything they say and do in cyberspace can be tracked and recorded, they may experience anxiety, mistrust, and even paranoia about being online.

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

ONLINE IDENTITY

Online identity, online personality or internet persona, is a social identity that an Internet user establishes in online communities and websites. It may also be an actively constructed presentation of oneself. A social network profile, a forum account, a video game character, or even a shopping cart can all be considered an online identity.

As a result, an Internet identity can be made up of items like:

- Login information
- Transactions on the internet
- Searching on the internet
- Previous medical history
- Year of birth
- History of browsing
- Profile photo
- Profile name

Ways to protect online Identity

1. Use Strong Passwords

   To make the passwords strong and difficult to guess, use combination of numbers, letters, and special characters. Passwords should not be obvious, such as your birth date or the name of your dog. Obviously, do not reveal your password to anybody else, and do not write it down in plain text. To save numerous passwords, use encrypted software such as KeePass / KeePassCT

2. Have Multiple Email Addresses

   For stuff like newsgroups, video games, and forums, it's best not to use your mail email address. Your primary email address should only be shared with people you know.

3. Use VPN

   A virtual private network (VPN) is a service that helps you secure your online identity by encrypting your personal data, protecting your internet traffic, and preventing online monitoring..

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Furthermore, a VPN may hide your genuine IP address, thereby assuring that no website can trace your true geo-location – and that no one can log any sensitive data related to your IP address.

ONLINE RELATIONSHIP

An internet relationship is a relationship between people who have met online, and in many cases know each other only via the Internet

The major difference here is that an internet relationship is sustained via computer or online service, and the individuals in the relationship may or may not ever meet each other in person. Otherwise, the term is quite broad and can include relationships based upon text, video, audio, or even virtual character. This relationship can be between people in different regions, different countries, different sides of the world, or even people who reside in the same area but do not communicate in person.

Types of Online Relationship

- **Dating website innovations**

Although the availability of uploading videos to the internet is not a new innovation, it has been made easier since 2008 thanks to YouTube. YouTube began the surge of video streaming sites in 2005 and within three years, smaller web developers started implementing video sharing on their sites. Internet dating sites have benefitted greatly since the surge in easiness and accessibility of picture and video uploading. Videos and pictures are equally important for most personal profiles. These profiles can be found on sites used for interpersonal relationships other than dating as well.

- **Social networking relationships**

Social networking has enabled people to connect with each other via the internet. Sometimes, members of a social networking service do know all, or many of their "friends" (Facebook) or "connections" (LinkedIn) etc. in person. However, sometimes internet relationships are formed through these services, including but not limited to: Facebook, Myspace, Google Plus, LinkedIn, Twitter, and Discord.

"Social networking service" is a very broad term, branching out to websites based on many different aspects. One aspect that is possible on all social networking sites is the possibility of an internet relationship. These sites enable users to search for new connections based on location, education, experiences, hobbies, age, gender, and more. This allows individuals meeting each other to already have some characteristic in common

- **Online gaming**

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Online gaming elicits the introduction of many different types of people in one interface. A common type of online game where individuals form relationships is the MMORPG, or a massively multiplayer online role-playing game. Some examples of MMORPG, Ever Quest, Second Life, Final Fantasy Online, and Minecraft . These games enable individuals to create a character that represents them and interact with other characters played by real individuals, while at the same time carrying out the tasks and goals of the actual game.

- **Online forums and chatrooms**

An Internet forum is a website that includes conversations in the form of posted messages. Forums can be for general chatting or can be broken down into categories and topics. They can be used to ask questions, post opinions, or debate topics. Forums include their own jargon, for example a conversation is a "thread". Different forums also have different lingo and styles of communicating.

There are religion forums, music forums, car forums, and countless other topics. These forums elicit communication between individuals no matter the location, gender, ethnicity, etc. although some do include age restrictions. Through these forums people may comment on each other's topics or threads, and with further communication form a friendship, partnership, or romantic relations

PERSONALITY TYPES IN CYBER SPACE

The personality styles discussed are:

psychopathic (antisocial)

narcissistic

schizoid

paranoid

depressive and manic

Sexual Masochism

histrionic

dissociative

1. **Psychopathic**

Antisocial personality disorder, sometimes called sociopathy, is a mental health condition in which a person consistently shows no regard for right and wrong and ignores the rights and feelings of others. People with antisocial personality disorder tend to purposely make others angry or upset and manipulate or treat others harshly or with cruel indifference. They lack remorse or do not regret their behaviour.

2. **Narcissistic personality**

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Narcissistic personality disorder is a mental health condition in which people have an unreasonably high sense of their own importance**.** Real narcissists aren't the ones taking selfies – they are often the ones bullying, harassing, and stalking others in cyberspace. perhaps the *least* surprising behavior narcissists engage in online is cyberbullying and trolling. Narcissists online enjoy bullying others and derive a sadistic sense of pleasure in doing so. They post provocative comments, disturbing threats, and cruel insults

3. **Schizoid personality**

Schizoid personality disorder (SPD) is a chronic and pervasive condition characterized by social isolation and feelings of indifference toward other people. People who have this disorder are often described as distant or withdrawn. They have limited social expression and tend to avoid social situations that involve interaction with other people.

4. **Paranoid Personality**

Paranoid personality disorder (PPD) is a mental illness characterized by paranoid delusions, and a pervasive, long-standing suspiciousness and generalized mistrust of others.

- Difficulty maintaining personal relationships
- Difficulty working in a social setting
- Loss of employment
- Development of psychotic illnesses

5. Depressive and Manic

Bipolar disorder, formerly called manic depression, is a mental health condition that causes extreme mood swings that include emotional highs (mania or hypomania) and lows (depression).

When you become depressed, you may feel sad or hopeless and lose interest or pleasure in most activities. When your mood shifts to mania or hypomania (less extreme than mania), you may feel euphoric, full of energy or unusually irritable. These mood swings can affect sleep, energy, activity, judgment, behavior and the ability to think clearly.

Episodes of mood swings may occur rarely or multiple times a year. While most people will experience some emotional symptoms between episodes, some may not experience any.

6. **Sexual Masochism Disorder**

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Sexual masochism disorder (SMD) is the condition of experiencing recurring and intense sexual arousal in response to enduring moderate or extreme pain, suffering, or humiliation

7. Histrionic Personality Disorder

Histrionic personality disorder (HPD) is defined by the American Psychiatric Association as a personality disorder characterized by a pattern of excessive attention-seeking behaviours, usually beginning in early adulthood, including excessive desire for approval. People diagnosed with the disorder are said to be lively, dramatic, enthusiastic, extroverted and flirtatious.

Histrionic personality disorder usually begins in your late teens or early 20s.A person with histrionic personality disorder may:

- Feel underappreciated or depressed when they're not the centre of attention.
- Have rapidly shifting and shallow emotions.
- Be dramatic and extremely emotionally expressive, even to the point of embarrassing friends and family in public.
- Have a "larger than life" presence.

8. Dissociative Disorder

Dissociative disorders are mental disorders that involve experiencing a disconnection and lack of continuity between thoughts, memories, surroundings, actions and identity. People with dissociative disorders escape reality in ways that are involuntary and unhealthy and cause problems with functioning in everyday life.

Computer and Cyber Addiction

Cyber addiction is the excessive, compulsive non-productive use of the Internet by an individual desperately relying on it to occupy free time for recreation or social purposes. It is often fueled by the overuse and lack of time regulation in online gaming and/or the use of mobile apps and social media networks.

Excessive Internet use has not been recognized as a disorder by the World Health Organization, the Diagnostic and Statistical Manual of Mental Disorders (DSM-5) or the International Classification of Diseases *(ICD-11)*. However, the diagnosis of gaming disorder has been included in the *ICD-11*. While you can experience these instincts with a laptop or even desktop computer, the size and convenience of smartphones and tablets means that we can take them just about anywhere and fulfil our urges of using the Internet.

Causes of Cyber Addiction

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

- abnormalities in neurochemical processes
- history of mental illness or a personality disorder
- personal or family history of addiction
- Internet access and availability

The following symptoms are typical of online addicts:

● Feelings of guilt

● Anxiety

● Depression

● Dishonesty

● Euphoric feelings when in front of the computer

● Unable to keep schedules

● No sense of time

● Isolation

● Defensiveness

● Avoiding doing work

● Agitation

Physical Symptoms of Online Addiction

The following symptoms are characteristic of someone who uses the computer for a very long period of time:

● Backache

● Headaches

● Weight gain or loss

● Disturbances in sleep

● Carpal tunnel syndrome

● Blurred or strained vision

Ms.Elakiya.V.,M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Short-Term and Long-Term Effects of an Online Addiction

The short-term effects of an online addiction include unfinished tasks ,forgotten responsibilities and weight gain.

Long-term effects

Long term effects are seen more in the physical symptoms such as backache, neck pain, and vision problems from staring at the screen. It can also lead to especially if the time spent online is focused on shopping, gambling and gaming

Carpel Tunnel Syndrome: Carpal tunnel syndrome is caused by pressure on the median nerve. The carpal tunnel is a narrow passageway surrounded by bones and ligaments on the palm side of the hand. When the median nerve is compressed, symptoms can include numbness, tingling, and weakness in the hand and arm.

Mrs.Elakiya.V., M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

UNIT II

CRIMES IN CYBER SPACE

Crimes: Types of Cyber Crimes–Reason for Cyber Crimes – Classification of Cyber Crimes –Cyber Laws in India–Prevention of Cyber Crimes –Tips for Avoiding Computer Crime Cyber crimes

Cyber crimes

A generalized definition of cybercrime may be unlawful acts wherein thecomputer is either a tool or target or both

Types of Cyber Crimes

Assault by threat- threating a person with fear for their lives or their families or person whose safety they are responsible for (such as employees or munities)through the use of a computer network such a email, videos, or phones.

Child Pornography - the use of computer networks to create, distribute, or access materials that sexually exploit underage children. Cyber Contents transferring illegal items through the internet that is banned in some locations.

Cyber laundering - electronic transfer of illegally obtained money with thegoal of hiding its source and possibly its destination.

Cyber stalking - express or implied physical threats that creates fear through the use of computer technology such as email, phones, text messages, webcams,websites or videos

Cyber terrorism - premeditated, usually politically motivated violence committed against civilians through the use of, or with the help of, computertechnology.

Cyber theft- using a computer to steal. This includes activities related to: breaking and entering, identity theft, fraud, hacking, plagiarism,and . Examples include:

1. Advertising or soliciting prostitution through the internet: It is against the lawto access prostitution through the internet (including in the state of Nevada in the United States) because the process of accessing the internet crosses state andsometimes national borders.

2. Drug Sales: Both illegal and prescription drug sales through the internet areillegal except as a customer through a state licensed pharmacy based in the United States.

Mrs.Elakiya.V., M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Online Gambling - Gambling over the internet a violation of American law because the gambling service providers require electronic payment for gamblingthrough the use of credit cards, debit cards, electronic fund transfers which is illegal with the Unlawful Internet Gambling Enforcement Act.

Cybertresspass- someone accesses a computer's or network's resources without the authorization or permission of the owner but does not alter, disturb, misuse, or damage the data or system. This is hacking for the purpose of entering an electronic network without permission. Examples might include:

1. Using a wireless internet connection at a hotel at which you are staying andaccessing the hotel private files without disturbing them because they are available.

2. Reading email, files, or noting which programmes are installed on a third-party's computer system without permission just for fun, because you can

This is sometimes called Snooping.

Cyber vandalism - Damaging or destroying data rather than stealing or misusing them (as with cyber theft) is called cyber vandalism. This can include a situation where network services are disrupted or stopped. This deprives the computer/network owners and authorized users (website visitors, employees) ofthe network itself and the data or information contained on the network Examples:

• Entering a network without permission and altering, destroying, or deletingdata or files.

• Deliberately entering malicious code (viruses) into a computer network to monitor, follow, disrupt, stop, or perform any other action withoutthe permission of the owner of the network.

Attacking the server of the computer network, so the server does not performproperly or prevents legitimate website visitors from accessing the network resources with the proper permissions.

Mrs.Elakiya.V., M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Reasons for Cyber Crime

- **Capacity to Store Data in Comparatively Small Space**

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.

- **Easy to Access**

The problem encountered in guarding a computer system from unauthorizedaccess is that there is every possibility of breach not due to human error but dueto the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders, retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

- **Complex**

The computers work on operating systems and these operating systems inturn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

- **Negligence**

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and controlover the computer system.

- **Loss of evidence**

Loss of evidence is a very common and obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent alsoparalyses this system of crime investigation.

Mrs.Elakiya.V., M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Classifications

1. Against Individuals
- their person
- their property of an individual

2. Against Organization
- Government and
- Firm, Company, Group of Individuals.

3. Against Society at large

The following are the crimes, which can be committed against the followingsgroup

Against Individuals:

i. Harassment via e-mails.
ii. Cyber-stalking.
iii. Dissemination of obscene material.
iv. Defamation.
v. Unauthorized control/access over computer system.
vi. Indecent exposure
Email spoofing
vii. Cheating and Fraud

Against Individual Property:

i. Computer vandalism.
ii. Transmitting virus.
iii. Unauthorized control access over computer system
iv. Intellectual Property crimes

Against Organization:

i. Unauthorized control access over computer system
ii. Possession of unauthorized information.
iii. Cyber terrorism against the government organization
iv. Distribution of pirated software etc.

Mrs.Elakiya.V., M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Against Society at large:

i. Pornography (basically child pornography)
ii. Polluting the youth through indecent exposure
iii. Trafficking
iv. Financial crimes
v. Sale of illegal articles
vi. Online gambling

Cyber laws in India

Cybercrimes can involve criminal activities that are traditional in nature, such astheft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code.

Primary sources of cyber law in India is the information Technology(ICT, 2000)

The purpose of ICT to provide Legal Recognition to electronic Commercy and to facilitate filing of electronic records with government.

Penalty Compensation and offences

- Section 43-5 : If any person without permission of owner or any other person who is in charge of computer – Then he shall be liable to pay damage.
- Section 66- If a Person portray a Dishonesty or fraud regarding cyber crime he or she will be Jailed for three years
- Unauthorized Access: Section 43(a): Access to memory, logical function Remotely shutting down computer by SMS -

Needs and Importance of Cyber Law

✓ Tackling Cyber Crime

✓ Successful And Smooth Functioning of E Commerce And Virtual Communication

✓ No Jurisdictional Boundaries

✓ Increasing Use Of Mobile Banking and Internet Banking

Mrs.Elakiya.V., M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Prevention of Cyber Crime

Prevention is always better than cure. It is always better to take certain precaution while operating the net.

Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cybercrime Cell, advocates the **5P'S** mantra for online security:

1. Precaution,
2. Prevention,
3. Protection,
4. Preservation
5. Perseverance.

A netizen should keep in mind the following things
Given its prevalence, you may be wondering how to stop cybercrime? Here are some sensible tips to protect your computer and your personal data from cybercrime:

1. Keep software and operating system updated

Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.

2. Use anti-virus software and keep it updated

Using anti-virus or a comprehensive internet security solution like Kaspersky Total Security is a smart way to protect your system from attacks. Anti-virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you piece of mind. Keep your antivirus updated to receive the best level of protection.

3. Use strong passwords

Be sure to use strong passwords that people will not guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this easier.

Mrs.Elakiya.V., M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

4. Never open attachments in spam emails

A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know. Do not click on links in spam emails or untrusted websites

Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.

5. Do not give out personal information unless secure

Never give out personal data over the phone or via email unless you are completely sure the line or email is secure. Make certain that you are speaking to the person you think you are.

6. Contact companies directly about suspicious requests

If you are asked for personal information or data from a company who has called you, hang up. Call them back using the number on their official website to ensure you are speaking to them and not a cybercriminal. Ideally, use a different phone because cybercriminals can hold the line open. When you think you've re-dialed, they can pretend to be from the bank or other organization that you think you are speaking to.

7. Be mindful of which website URLs you visit

Keep an eye on the URLs you are clicking on. Avoid clicking on links with unfamiliar or URLs that look like spam. If your internet security product includes functionality to secure online transactions, ensure it is enabled before carrying out financial transactions online.

8. Keep an eye on your bank statements

Spotting that you have become a victim of cybercrime quickly is important. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

Mrs.Elakiya.V., M.Sc
Assistant Professor
Department of Psychology
DKM College for Women (Autonomous)

Tips for avoiding computer crime

1. Keep up to date on major security breaches

If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.

2. Take measures to help protect yourself against identity theft

Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. You might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That's why it's important to guard your personal data. A VPN — short for virtual private network — can also help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

3. Know that identity theft can happen anywhere

It's smart to know how to protect your identity even when traveling. There are a lot of things you can do to help keep criminals from getting your private information on the road. These include keeping your travel plans off social media and being using a VPN when accessing the internet over your hotel's Wi-Fi network.

4. Keep an eye on the kids

Identity thieves often target children because their Social Security number and credit histories frequently represent a clean slate. You can help guard against identity theft by being careful when sharing child's personal information. It's also smart to know what to look for that might suggest your child's identity has been compromised.

5. Know what to do if you become a victim

If you believe that you've become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the Federal Trade Commission of US Government . This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to defeat

criminals from taking advantage of other people in the future. If you think cybercriminals have stolen your identity. These are among the steps you should consider.

- Contact the companies and banks where you know fraud occurred.
- Place fraud alerts and get your credit reports.
- Report identity theft to the FTC.

6.Use a full-service internet security suite

It's a good idea to consider trusted security software like Norton 360 with LifeLock Select, which provides all-in-one protection for your devices, online privacy, and identity, and helps protect your private and financial information when you go online.

7.Use strong passwords

Don't repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 10 letters, numbers, and symbols. A password management application can help you to keep your passwords locked down.

8.Keep your software updated

This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.

9. Manage your social media settings

Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better. For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

UNIT III

CYBER BULLYING

Meaning - History of Cyber Bullying – Types of Cyber Bullying –Signs of Cyber Bullying –Effects of Cyber Bullying –Cyber Bullying Vs School Yard Bullying –Prevention Tips for Bullying: Middle School, Teenagers– Suggestion for Parents.

DEFINITION

- Cyberbullying is "an aggressive, intentional act or behaviour that is carried out by a group or an individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself."

MEANING

- **Bullying**, in general, refers to the act of deliberately and repeatedly targeting someone with hurtful or harmful behaviour, often with the intention of causing emotional, psychological, or physical distress
- **Cyberbullying** or **cyberharassment** is a form of bullying or harassment using electronic means.
- Cyberbullying and cyberharassment are also known as online bullying. It has become increasingly common, especially among teenagers and adolescents, due to the communication technology advancements

HISTORY OF CYBER BULLYING

The history of cyberbullying is closely tied to the development and proliferation of digital technology and the internet. Here's a brief overview of its history:

1. **Early Internet Era (1990s - 2000s):**
   Cyberbullying first emerged with the rise of online communication tools and social media platforms in the late 20th century. In the early days of the internet, it primarily involved in
   - ✓ sending mean-spirited emails,
   - ✓ spreading rumors on online forums, and
   - ✓ engaging in hurtful chatroom conversations.
2. **Text Messaging and Cell Phones:**
   As mobile phones became more common in the early 2000s, text messaging became a new avenue for cyberbullying. Individuals could send hurtful messages to others, often anonymously.
3. **Social Media and Web 2.0 (Mid-2000s - Present):**

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

The advent of Web 2.0 and the rapid expansion of social media platforms like Facebook, Twitter, and Instagram introduced new opportunities for cyberbullying.

Perpetrators could now

- ✓ create fake profiles,
- ✓ post hurtful comments,
- ✓ share embarrassing photos or videos, and
- ✓ launch coordinated attacks on victims.

4. **Anonymous Online Platforms (2000s - Present):**
   Websites and forums that allow users to post content anonymously, such as various comment sections on news sites, have been hotspots for cyberbullying. Anonymity often put individuals to engage in more aggressive behavior.
5. **Laws and Regulations (2000s - Present)**: Governments and organizations worldwide have responded to cyberbullying by enacting laws and regulations to combat online harassment. These laws vary by jurisdiction but often include measures to punish cyberbullies and protect victims.
6. **Increased Awareness and Anti-Bullying Campaigns (2000s - Present)**: As the severity and prevalence of cyberbullying have become more evident, there has been a global push to raise awareness about the issue. Schools, parents, and organizations have launched anti-bullying campaigns to educate people about the consequences of cyberbullying and encourage online civility.
7. **Social Media Moderation and Reporting Tools (2010s - Present):** Social media platforms have implemented moderation policies and reporting tools to help users combat cyberbullying. This includes options to report abusive content and block or mute users.

TYPES OF CYBER BULLYING

It's essential to recognize the various forms of cyberbullying and take steps to prevent and address them to create a safer and more respectful online environment. It can manifest in various ways, often involving the use of technology and social media platforms. Here are some common types of cyberbullying:

1. **Harassment:** Sending threatening, hurtful, or offensive messages repeatedly to an individual, often with the intent to intimidate or upset them.
2. **Impersonation:** Pretending to be someone else online, often by creating fake social media profiles or using someone else's identity to post hurtful or embarrassing content.
3. **Outing:** Sharing someone's private or personal information, such as photos, messages, or secrets, without their consent to embarrass or harm them.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

4. **Exclusion**: Deliberately leaving someone out of online groups, chats, or activities, or spreading rumors to isolate them socially.
5. **Cyberstalking:** Engaging in persistent, unwanted online attention or following someone's online activity closely with the intent to cause fear, discomfort, or harm.
6. **Doxing:** Revealing an individual's private or personal information, such as their address, phone number, or workplace, online without their consent, often with malicious intent.
7. **Trolling**: Posting provocative or offensive comments or content online to provoke reactions and disrupt online discussions or communities.
8. **Flaming:** Using derogatory language, insults, or hate speech towards someone based on their race, religion, gender, sexual orientation, or other personal characteristics.
9. **Catfishing:** Creating a fake online persona to deceive and manipulate others, often for personal gain or to emotionally harm the victim.
10. **Revenge Porn:** Sharing sexually explicit images or videos of someone without their consent, usually after a romantic relationship ends, with the intent to humiliate or harm the victim.
11. **Bystander Cyberbullying**: Although not directly involved, individuals who witness cyberbullying but do nothing to stop it or report it can also contribute to the harm by enabling the behavior.

SIGNS OF CYBER BULLYING

Recognizing the signs of cyberbullying is crucial for identifying when someone is being targeted online and taking steps to address the situation.

Here are some common signs that may indicate someone is experiencing cyberbullying:

1. **Emotional Distress:** The victim may show signs of emotional distress, such as increased anxiety, depression, anger, or withdrawal from social activities.
2. **Change in Behavior**: Sudden changes in behavior, mood, or routine may be indicative of cyberbullying. This can include a
    - ✓ decline in academic or work performance,
    - ✓ loss of interest in hobbies, or
    - ✓ a sudden reluctance to use the internet or social media.
3. **Avoidance of Technology**: Someone who is being cyberbullied may start avoiding their computer, phone, or other digital devices, as these tools remind them of the harassment.
4. **Isolation:** Victims may withdraw from friends and family, avoiding social interactions or gatherings, both online and offline.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

5. **Increased Screen Time:** Paradoxically, some victims may spend more time online, trying to monitor or respond to the cyberbullying, which can further increase their distress.
6. **Secretiveness:** They may become secretive about their online activities, passwords, or messages, as they fear the bullies might gain access to their accounts.
7. **Change in Sleep Patterns**: Cyberbullying can disrupt sleep patterns, leading to insomnia or excessive sleep.
8. **Decline in Self-Esteem:** Victims of cyberbullying often experience a decline in self-esteem and self-worth. They may express negative thoughts about themselves.
9. **Physical Symptoms:** Stress caused by cyberbullying can manifest in physical symptoms like headaches, stomach aches, or other stress-related ailments.
10. **Decline in Academic or Work Performance:** Cyberbullying can negatively impact one's ability to concentrate and perform well in school or at work.
11. **Social Withdrawal:** Victims may avoid social gatherings or online communities where they were previously active participants.
12. **Evidence of Harassment:** Look for signs of cyberbullying in the form of hurtful messages, emails, social media posts, or comments. Screenshots or copies of such messages may be evidence.
13. **Changes in Friendships:** Victims might lose friends or experience strained relationships due to the actions of cyberbullies or because they're targeted for associating with the victim.
14. **Self-Harm or Suicidal Thoughts**: In severe cases, cyberbullying can lead to self-harm or suicidal thoughts.

It's important to remember that these signs may not always be definitive proof of cyberbullying, as they can also indicate other issues or challenges a person may be facing.

However, if we notice these signs in someone, it's essential to approach them with empathy, offer support, and encourage open communication.

EFFECTS OF CYBER BULLYING

Cyberbullying can have significant and long-lasting effects on victims, both emotionally and psychologically.

It's important to recognize that the effects of cyberbullying can vary widely from person to person and depend on factors like the severity, duration, and frequency of the harassment, as well as the individual's resilience and support network.

Some of the common effects of cyberbullying include:

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

1. **Emotional instability:** Cyberbullying often leads to increased levels of emotional distress, such as anxiety, depression, and feelings of helplessness. Victims may experience intense sadness, fear, or anger.
2. **Low Self-Esteem:** Repeated online harassment and negative comments can erode a person's self-esteem and self-worth, causing them to doubt themselves and their abilities.
3. **Social Isolation**: Many victims of cyberbullying withdraw from social interactions, both online and offline, to avoid further harassment. This isolation can lead to feelings of loneliness and alienation.
4. **Low performance at work or education**: The emotional toll of cyberbullying can result in difficulties at school or work, including a decline in academic or job performance.
5. **Physical Health Issues**: Stress and anxiety caused by cyberbullying can manifest as physical health problems, such as headaches, stomach aches, and sleep disturbances.
6. **Cyber Addiction**: Some victims may develop unhealthy coping mechanisms, such as excessive internet use or dependence on social media, to escape their problems.
7. **Distrust of Others**: Victims of cyberbullying may develop a general distrust of people, both online and offline, which can impact their ability to form healthy relationships.
8. **Self-Harm and Suicidal Ideation**: In severe cases, cyberbullying can lead to self-harming behaviors or thoughts of suicide. It is essential to take any such statements seriously and seek immediate help.
9. **Post-Traumatic Stress Disorder (PTSD):** In some cases, the trauma from cyberbullying can lead to the development of PTSD, characterized by flashbacks, nightmares, and severe anxiety.
10. **Damaged Reputation**: Cyberbullying can damage a person's reputation, making it challenging to maintain personal and professional relationships.
11. **Cyberbullying Endurance**: Some victims of cyberbullying may, in turn, become bullies themselves as a way of coping with their own trauma, that gives way to continue the bullying.
12. **Financial and Legal Consequences**: In certain cases, cyberbullying incidents can have legal and financial consequences for both the victim and the perpetrator, especially when it involves the dissemination of private or sensitive information.

CYBER BULLYING Vs SCHOOL YARD BULLYING

Cyberbullying and schoolyard (or traditional) bullying share some similarities, such as the intent to harm, intimidate, or humiliate the victim, but they differ in several key ways due to the medium and context in which they occur. Here are some of the primary differences between cyberbullying and schoolyard bullying:

TITLE	CYBER BULLYING	SCHOOL YARD BULLYING

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

Medium of Communication	Occurs **online** or through digital communication channels, such as social media, emails, text messages, or online forums	Takes place in **physical settings**, typically within or around the school campus, such as classrooms, hallways, playgrounds, or school buses
Anonymity and Distance	Criminal can remain **anonymous or hide their identity,** making it easier to harass the victim from a distance.	Bullying is usually **face-to-face**, with the perpetrator and victim often knowing each other's identities.
24/7 Accessibility:	Can **occur at any time**, day or night, as long as the victim and perpetrator have internet access and devices.	Typically **confined to school hours** and the immediate vicinity of the school
Permanence and spread	Content **shared online can be permanent and easily spread to a wider audience**, potentially causing long-lasting damage	Often **remains within the immediate witnesses**, and evidence tends to be limited to those who were present.
Potential Audience	Has the potential **to reach a larger and more widespread audience**, as posts, messages, or images can be shared or forwarded	Usually **limited to a smaller group of peers or onlookers** within the school environment.
Psychological Impact	Can have a **significant psychological impact due to the potential for a 24/7 barrage of harassment**, which may be more challenging for victims to escape.	While also emotionally damaging, it may offer some relaxation when students are not at school.
Physical vs. Emotional	Primarily involves emotional and psychological harassment, although it can escalate to physical threats or harm in some cases.	Can encompass **physical aggression, verbal abuse, and social exclusion**, in addition to emotional harm.
Reporting and Evidence	**Leaves digital traces, which can be easier to document and report**, but it may also involve more complex investigations to identify the perpetrators	**Can be witnessed by school staff or students**, making it more straightforward to report but potentially **more challenging to address when adults are not present**.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

It's important to recognize that both forms of bullying can be harmful and have serious consequences for victims.

Schools, parents, and communities should take proactive measures to prevent and address both cyberbullying and schoolyard bullying, fostering safe and respectful environments for all individuals, both online and offline

PREVENTION TIPS FOR BULLYING: MIDDLE SCHOOL

Preventing bullying in middle school is essential to create a safe and supportive learning environment.

Middle school students are at an age where they are developing social skills and independence, making it crucial to address bullying effectively. Here are some specific tips for preventing bullying in middle schools:

1. **Educate Students**:
   - ✓ Conduct regular anti-bullying programs and workshops that teach students about the different forms of bullying, its effects, and how to prevent it.
   - ✓ Promote the idea that kindness, empathy, and inclusion are values to uphold.
2. **Promote Open Communication**: Create an environment where students feel comfortable discussing their concerns with trusted adults, such as teachers, counselors, or school staff.
   Encourage students to report bullying incidents promptly, and assure them that their reports will be taken seriously and kept confidential.
3. **Establish a Zero-Tolerance Policy**: Develop and enforce a clear anti-bullying policy that outlines consequences for bullying behavior. Make sure all students and parents are aware of this policy.
4. **Provide Bystander Training**: Teach students how to be active bystanders and intervene safely when they witness bullying. Encourage them to support the victim and report incidents.
5. **Create Safe Reporting Mechanisms**: Establish anonymous reporting systems, such as suggestion boxes or online forms, to enable students to report bullying without fear of retaliation.
6. **Cyberbullying Awareness:** Address the issue of cyberbullying explicitly, educating students about responsible online behavior and the potential consequences of their actions.
7. **Classroom Activities**: Incorporate anti-bullying themes into the curriculum, including discussions, group activities, and projects that promote empathy and understanding.
8. **Social-Emotional Learning (SEL**): Integrate SEL programs into the school curriculum to help students develop social and emotional skills, such as self-awareness, self-regulation, and relationship-building.
9. **Parental Involvement**: Engage parents in anti-bullying efforts by holding informational meetings, workshops, or seminars on bullying prevention and how to support their children.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

10. **Peer Mediation Programs**:Establish peer mediation programs that empower students to resolve conflicts peacefully and constructively.
11. **Support for Victims:** Provide counselling and support services for victims of bullying to help them cope with the emotional impact and build resilience.
12. **Role Modeling**: Encourage teachers, staff, and administrators to model respectful behavior, empathy, and conflict resolution skills for students.

Preventing bullying in middle school requires a comprehensive, proactive approach involving students, educators, parents, and the community. By fostering a culture of respect and empathy and equipping students with the tools to prevent and address bullying, middle schools can create a safer and more inclusive learning environment.

PREVENTION TIPS FOR BULLYING: TEENAGERS

Preventing cyberbullying is a collective effort that involves teenagers taking responsibility for their online behavior and promoting a respectful online environment.

Here are some tips and strategies for teenagers to prevent cyberbullying:

- **Be Mindful of Online Behavior**: Treat others online with kindness and respect. Thinking before post or share anything online, considering how it might impact others.
- **Secure Passwords**: Use strong, unique passwords for online accounts and change them regularly.
- Avoid sharing passwords with anyone, even friends would help to reduce harassment.
- **Recognize the Signs of Cyberbullying**: Be aware of the signs of cyberbullying, whether the teenager is the victim, bystander, or even the perpetrator.
- **Don't Forward Hurtful Messages or Content**: Refuse to participate in cyberbullying by not forwarding or sharing hurtful messages, images, or rumors.
- **Be an Upstander, not a Bystander**: If any teenager witness cyberbullying, stand up for the victim and support them. Report the bullying to the appropriate authorities or platform administrators.
- **Monitor Online Reputation**: Teenager should Google periodically to see what information about them is available online. Be proactive about removing any harmful or inappropriate content associated with your name.
- **Limit Screen Time**: Balance one online and offline activities to maintain a healthy lifestyle and prevent overexposure to potentially harmful online interactions.
- **Avoid Responding Immediately**: If any teenager experience cyberbullying, he/she should resist the urge to retaliate or respond with anger. It can escalate the situation. ***Instead, document the harassment and report it to adults or authorities.***

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

- **Seek Support from Trusted Adults**: Talk to a parent, guardian, teacher, school counsellor, or other trusted adult who can provide guidance and help address the situation effectively.
- **Educate oneself**: Stay informed about the latest online safety tips and resources for dealing with cyberbullying.
- **Report and Block**: Use the reporting and blocking features on social media platforms to protect yourself from cyberbullying. Report any harassing content or messages to the platform administrators.

PREVENTION TIPS FOR BULLYING: SUGGESTION FOR PARENTS

Preventing bullying involves a collaborative effort between parents, schools, and communities. Here are some suggestions for parents to help prevent bullying and support their children:

- **Open Communication:** Maintain open and honest communication with your child. Encourage them to share their experiences, both positive and negative.
- **Educate Your Child**: Teach your child about the different forms of bullying, how to recognize it, and what to do if they experience or witness bullying.
- **Set a Good Example**: Model respectful behaviour, empathy, and conflict resolution skills in your own interactions with others.
- **Monitor Online Activity**: Be aware of your child's online activity, including social media use, and discuss responsible online behaviour. Set rules and guidelines for internet and smartphone use.
- **Know the Signs:** Be aware of signs that your child may be a victim of bullying, such as changes in behavior, withdrawal, or declining academic performance.
- **Teach Conflict Resolution Skills**: Help your child develop effective conflict resolution skills, such as negotiation, compromise, and assertiveness.
- **Monitor Their Friends:** Be aware of your child's friends and social circle. Encourage positive friendships and discourage involvement with peers who may engage in bullying behavior.
- **Encourage Extracurricular Activities**: Support your child's participation in extracurricular activities and hobbies, which can boost self-esteem and provide opportunities for social interaction.
- **Report Cyberbullying:** If your child is a victim of cyberbullying, document the evidence and report it to the appropriate authorities, school officials, or social media platforms.
- **Stay Informed:** Keep yourself informed about your child's school's policies and procedures regarding bullying prevention and reporting.
- **Seek Professional Help if Needed**: If your child is experiencing severe emotional distress due to bullying, consider seeking the assistance of a mental health professional.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

- **Community Involvement**: Engage community organizations, local government, and businesses in anti-bullying initiatives.
- **Technological boundaries should be set:** Cyberbullying is a concern, with most Children having access to tablets, cell phones, and computers nowadays. Make sure your child's computer has the proper age-appropriate filter. Add them as friends on Twitter, Instagram, Snapchat, or Facebook, so youcan see what is happening.

Preventing bullying requires ongoing vigilance and support from parents. By actively engaging with your child, promoting empathy and communication, and working collaboratively with schools and communities, you can help create a safer environment for your child and others.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

UNIT IV

CYBER STALKING AND TRAFFICKING

Cyber Stalking: Meaning - Types of Stalking – Motives of Cyber Stalkers – Types of Stalkers –Preventive Measures. Cyber Trafficking: Meaning –Components of Trafficking – Purpose of Trafficking –Current Trends in Trafficking - Preventive Measures and Help Line.

DEFINITION:

- Cyberstalking refers to the act of using digital communication tools and technologies to harass, threaten, or intimidate someone.
- **Cyberstalking** is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.

MEANING:

- It involves the persistent and unwanted pursuit of an individual online, often with malicious intent. Cyberstalkers may use various online platforms such as social media, email, instant messaging, or other means to engage in this behavior.
- It may include false accusations, defamation, slander and libel.
- It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, doxing, or blackmail.

TYPES OF STALKING

A. **Harassment:** This involves sending repeated, offensive, or threatening messages to the victim via email, social media, text messages, or other online platforms. Harassment can also include hate speech, name-calling, or spreading false information about the victim.

B. **Doxxing:** Cyberstalkers may engage in doxxing by revealing and sharing the victim's personal information, such as their home address, phone number, workplace, or financial details, often with malicious intent.

C. **Stalking through Social Media**: Stalkers can use social media platforms to monitor the victim's online presence, engage in unwanted contact, and even manipulate their online relationships.

D. **Phishing:** Cyberstalkers may use phishing emails or messages to trick the victim into revealing sensitive information, such as login credentials or financial details, which can then be used for malicious purposes.

E. **Hacking and Surveillance**: In some cases, cyberstalkers may gain unauthorized access to the victim's email accounts, social media profiles, or devices to monitor their activities or steal personal information.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

F. **Monitoring through Spyware or Malware**: Some cyberstalkers use malicious software (spyware or malware) to gain unauthorized access to the victim's devices, emails, or online accounts. This allows them to monitor the victim's online and offline activities.

G. **Online Tracking:** Cyberstalkers may use various online tracking methods to follow the victim's physical movements, such as tracking their smartphone's location, following their social media check-ins, or monitoring their online purchases.

H. **Economic Cyberstalking**: In some cases, cyberstalkers may attempt to harm the victim financially by hacking into their bank accounts, stealing their identity, or engaging in financial fraud.

MOTIVES OF CYBER STALKERS

- **A stalker is an individual who engages in a pattern of unwanted and often obsessive behavior directed towards another person, causing that person to feel harassed, threatened, or fearful.**

Cyberstalkers engage in online harassment and intimidation for various motives, and understanding these motives can help victims and law enforcement address the issue more effectively. Motives can vary widely among cyberstalkers, and they often exhibit a combination of several factors. Some common motives for cyberstalking include:

a) **Revenge:** Cyberstalks may seek revenge for perceived slights or grievances. This could include former romantic partners seeking revenge after a breakup, ex-employees with a grudge against their former employer, or individuals seeking retaliation for real or imagined offenses.

b) **Obsession:** Some cyberstalks become obsessed with their victims, often due to an unrequited romantic interest or a fixation on a celebrity or public figure. Their obsession drives them to engage in persistent online harassment.

c) **Control and Dominance**: Cyberstalks may have a need for control and dominance over their victims. They derive satisfaction from exerting power over someone else's life, often attempting to dictate their actions and decisions.

d) **Jealousy and Envy**: Envy and jealousy can motivate cyberstalks to target individuals who possess qualities, possessions, or relationships they covet. They may harass and attempt to damage the reputation of those they envy.

e) **Entertainment and Amusement**: Some individuals engage in cyberstalking purely for entertainment purposes or as a form of trolling. They find pleasure in causing distress to their victims or creating chaos online.

f) **Mental Health Issues:** In some cases, cyberstalks may have underlying mental health issues, such as delusions or personality disorders, which drive their obsessive and harmful online behaviours.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

g) **Financial Gain:** Certain cyberstalks may engage in online scams, identity theft, or fraud as a means to achieve financial gain. They may use cyberstalking tactics to gather personal information for these illicit activities.

h) **Political or Ideological Motives**: In the context of political or ideological conflicts, cyberstalks may target individuals or groups who hold opposing views. They may use online harassment as a means to intimidate or silence those with differing opinions.

i) **Sexual Gratification**: Some cyberstalks engage in sextortion or other forms of sexual harassment to satisfy their own desires. They may pressure victims into sending explicit images or engaging in sexual conversations under threat.

j) **Sadism:** In extreme cases, cyberstalks exhibit sadistic tendencies, deriving pleasure from inflicting emotional or psychological pain on their victims. Their actions can be especially harmful and relentless.

TYPES OF STALKERS

Types of Stalkers	Characteristics	Motives to put Victims in sufferings
DELUSIONAL STALKER	❖ a history of mental illnesses, usually untreated, such as schizophrenia, manic depression, or borderline personality disorder; but are not limited to a single psychological illness ❖ denial of their mental illnesses, to appear normal to the society ❖ form love to hate relationships with friends	A delusional stalker is usually a loner & often chooses victims who are married woman, a rity or doctors, teachers
INTIMATE STALKER	❖ The intimate stalker cannot accept that the relationship has ended and begin to stalk the partner the Internet. ❖ Mostly females ❖ Stalker tries to harm or win back the partner	Victim is put into suffering if they are forming a new love interest, communicate with someone or same sexual orientation
VENGEFUL STALKER	❖ The most dangerous and destructive types of Inte stalker ❖ **Use** obsessive stalking techniques, profane bullyin sexually explicit harassment ❖ most commonly linked to crimes beyond stal	Motive to cause misery to the victim, this type of stake may act to publicly shame or create falsifications to assassinate the character of

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

	which involve kidnapping, assaults, sexually motiv crimes against children, and even murder.	the victim
EROTOMANIC STALKER	❖ Form non-existent relationships with their victim. ❖ Stalkers believe their actions, of abuse, will i lead to the victim falling into love with them. ❖ The Erotomanic stalkers goal is to be loved, sexually fulfilled, or given attention they may resort to violence to get their wants, desires, and needs met.	❖ Suffers victim egotistical, self-centred and relationship with the friends and family.
TROLLING STALKER	❖ Victims to this type of Internet stalker can known individual or complete stranger. . ❖ Post comments obsessively violent to their victims; these comments may also be irrelevant, inflammatory, and off-topic	❖ Trolling stalkers wish death on their victims, steal content, mimic behaviours, copy actions, and threaten
PREDATORY STALKER	❖ Internet stalkers are classic sexual predators. ❖ Sexual predators pray on those de appear to be weaker usually females and children; and may engage in behaviours such as surveillance, monitoring internet activities, obscene phone calls, fetishism, voyeurism, sexual masochism, sexual sadism, and/or exhibitionism.	❖ predatory stalkers are motivated by the desire for sexual cation and power over the victim.

PREVENTIVE MEASURES TO AVOID CYBER STALKING

- Use public Wi-Fi carefully as it can be hacked easily.
- Use a virtual private network (VPN) to hide your IP address and other details.
- Do not keep your devices lying around carelessly as someone may take the opportunity to install spyware.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

- All devices should be password protected and updated regularly.
- Use anti-spyware.
- Always log out of online accounts.
- Beware of apps that want access to your Facebook or contacts list.

a) **Don't post personal information online**

Never post your **personal address, date of birth, phone number, or bank account details** anywhere online.Keep your account as private domain wher only friends and family see the informations.

b) Do an internet search of your own name

A good preventative measure is to **check whether there's personal information** about you online by Googling your own name.

c) Optimize your privacy settings

Most social media platforms have privacy settings like Instagram, Snapchat, Facebook, and Google accounts, you can protect yourself better online.

Make sure that you only accept friend requests from people you know and trust. **Disable your geo-location settings** on all your apps and devices.

d) Automatically install security updates

Devices like smartphones, computers, and tablets **regularly receive security or bug fixes**. Often, these are in response to a recent hacking strategy or new security vulnerabilities.

It's tempting to snooze or delay those updates until a more convenient time, but don't. The best thing to do is to **set all updates to install automatically**

e) Install antivirus

Antivirus software prevents these attacks, among other things, by doing a virus scan of your devices.
Hide your IP address by using a VPN
Another way to protect your identity from online criminals is to use a virtual private network (VPN) when you are browsing the internet. **A virtual private network hides your real IP address**.

f) Password-protect all your devices and accounts

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

Always use unique and secure passwords. If the person who stalks you is someone you know, it's easier for them to guess passwords. Create a strong password and change it regularly.

g) Take precautions after a bad break up

While you are not responsible for someone else's behavior, it can help to be extra careful online if you've recently had a bad breakup. If your ex-partner is **angry, abusive, or being difficult** in any way, make sure to change your passwords, including email, social media platforms, and bank accounts.

STEPS FOR A VICTIM TO TAKE TO PROTECT FROM CYBER STALKERS

CYBER TRAFFICKING

- Cyber-trafficking as a term covers instances where victims of human trafficking for sexual exploitation are trafficked or transported to so-called 'cybersex dens', where there are webcams and other electronic means that record and stream their exploitation.
- Cyber form of forced prostitution.[

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

- Victims are forced to perform sexual acts on themselves or other people in sexual slavery or raped by the traffickers or assisting assaulters in live videos. Victims are frequently ordered to watch the paying live distant consumers or purchasers on shared screens and follow their commands
- Women, children, and people in poverty are particularly vulnerable to coerced internet sex.

COMPONENTS OF TRAFFICKING

Internet-based trafficking has become increasingly varied; spanning from simple setups of advertising victims online, to traffickers' use of communications platforms to broadcast exploitation

a) **Recruitment:** The process of identifying and engaging potential victims of trafficking online. Traffickers often use social media, fake job offers, dating websites, or other online platforms to lure individuals into exploitative situations.

b) **Transportation:** In the context of cyber trafficking, transportation refers to the movement of victims across borders or regions using online communication and coordination. This may involve arranging travel documents or providing instructions for illegal border crossings.

c) **Harboring:** Cyber traffickers may use the internet to hide and shelter victims in remote locations or arrange for them to be housed in exploitative conditions, such as brothels, sweatshops, or agricultural facilities.

d) **Receipt:** The act of taking possession of a victim, which can involve meeting in person or coordinating online to initiate exploitation. For example, a trafficker may use online communication to instruct a victim to meet at a specific location.

e) **Internet exploitation**: The ultimate goal of cyber trafficking is to exploit the victims. This can take various forms, including forced labor, sexual exploitation, forced begging, or other forms of coerced labor or services.

f) **Online Advertising**: Traffickers often use websites, social media platforms, and online forums to advertise victims for exploitation. They may create and manage online advertisements for commercial sex, labor, or other services involving victims.

g) **Money Laundering**: Cyber traffickers may use

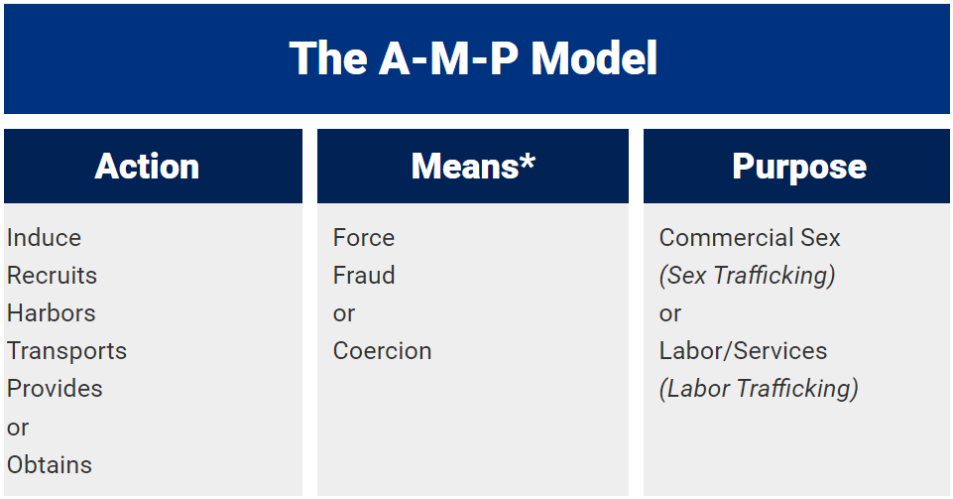
h) from their illegal activities. This could involve cryptocurrency transactions, online banking, or other digital financial methods to obscure the source of funds.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

i) **Technology and Communication Tools**: Cyber traffickers leverage technology and communication tools to carry out their activities. This includes smartphones, messaging apps, social media, and encryption to communicate with victims and other traffickers.

PURPOSE OF CYBER TRAFFICKING

- The purpose of cyber trafficking, like all forms of human trafficking, is to exploit vulnerable individuals for financial gain or other illicit purposes.
- Cyber trafficking involves using digital technology and the internet to recruit, transport, transfer, harbor, or receive individuals for the purpose of exploitation



a) Force, Fraud, or Coercion U.S. law defines human trafficking as the use of force, fraud, or coercion to compel a person into commercial sex acts or labor or services against his or her will.

b) Action-Means-Purpose: The Action-Means-Purpose (AMP) Model can be helpful in understanding the federal law. Human trafficking occurs when a perpetrator, often referred to as a trafficker, takes an Action, and then employs the Means of force, fraud or coercion for the Purpose of compelling the victim to provide commercial sex acts or labor or services

c) **Sexual Exploitation**: This includes activities such as sex trafficking, where victims are forced or coerced into engaging in commercial sexual acts against their will. Traffickers often advertise victims online for prostitution or sexual services.

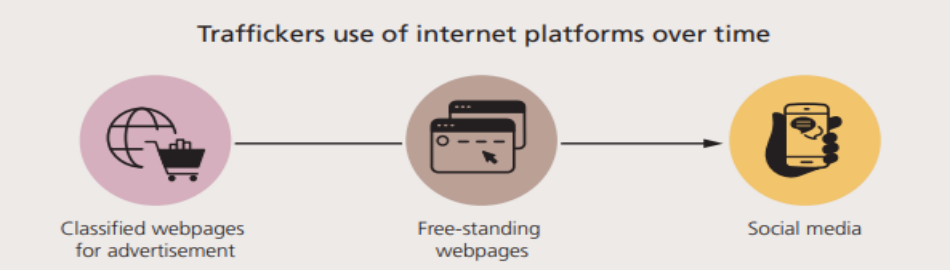
d) **Child Exploitation:** Cyber trafficking can target vulnerable children and adolescents, subjecting them to various forms of exploitation, including child labor, forced begging, or sexual exploitation. Online grooming and child exploitation material distribution can be part of this.

e) **Organ Trafficking:** In some cases, cyber trafficking can involve the illegal trade of human organs, where victims are forcibly or fraudulently coerced into selling their organs for transplantation.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

CURRENT TRENDS IN TRAFFICKING

Three broad typologies of platforms have been identified:



- **Social Media**

  Social media, including Facebook, Myspace, Skype, WhatsApp and Vkontakte. As technology-based trafficking has become more commonplace, social media has been increasingly used by traffickers, making this method of trafficking an emerging threat, especially for youth.
- **Classified webpages for advertisement**, referring to generic websites where individuals post advertisements or browse for items or services to buy or sell;
- **Free-standing webpages**, referring to websites created by traffickers that do not form part of larger domains. Online classified sites or free-standing webpages are more frequently used to post fake job listings with the purpose of recruiting victims, or to publicize the services offered by exploited victims
- **Cryptocurrency Transactions**: The use of cryptocurrencies like Bitcoin for transactions related to cyber trafficking has grown. Cryptocurrencies provide a level of anonymity that can make it difficult for law enforcement to trace financial transactions.
- **Non-consensual Image Sharing (Revenge Porn):** The sharing of non-consensual intimate images
- (revenge porn) remains a problem. Victims, especially women, are often targeted, and their explicit images are distributed without their consent.
- **Online Grooming**: Traffickers groom potential victims through online communication. This can involve building a relationship with the victim before exploiting them or manipulating them into meeting in person.
- **Dark Web and Encrypted Platforms**: Much of the activity related to cyber trafficking, including the sale of exploitative content and services, occurs on the dark web and encrypted messaging platforms, making it challenging for law enforcement to monitor and track.

PREVENTIVE MEASURES AND HELPLINE NUMBERS

PREVENTIVE MEASURES

I. **Law enforcement:**

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

Law enforcement must be thorough in investigating all instances of cyber-traffic. If more criminals are caught and get stricter sentences, less people would be incentivised in participating in such online sex trafficking rings. Thus, law enforcement must invest more resources, for example in technology and experts that can track criminals, even when they are hiding their location.

II. Awareness to channels or buyers:

Policy makers should also channel their efforts into tackling these difficult issues, for example by criminalising the seeking, purchasing and possession of sexual content which was created through illegal means.

III. Educating public:

The public must be better informed on these contemporary issues and must be aware how to recognise risks and who to signalise. It seems that whistle-blowers are incredibly important, as law enforcement is not always able to track down criminals on their own.

IV. Government resource restrictions:

Overall, governments should be keener on providing enough resources and support for marginalised groups, so they do not become easy victims for criminal who promise them money and a better life.

V. Online Safety:

Teach individuals, especially children and teenagers, about online safety and responsible internet use. Encourage them to be cautious when sharing personal information online.

Use privacy settings on social media platforms to control who can see your personal information and posts.

VI. Strong Passwords and Security:

Promote the use of strong, unique passwords for online accounts, and enable two-factor authentication where possible to protect against unauthorized access.

Regularly update software and security settings on devices to guard against malware and hacking attempts.

VII. **Report Suspicious Activity**:

Encourage individuals to report any suspicious online activity, grooming attempts, or messages to law enforcement and relevant authorities.

Platforms like social media networks often have mechanisms to report abusive or exploitative content.

VIII. Safe Online Relationships:

Teach individuals to be cautious when forming online relationships, especially with people they have not met in person.

Encourage open communication between parents, guardians, and children about their online interactions.

HELPLINE NUMBERS

Helpline numbers can vary by country and region, so I can provide some general guidelines for finding assistance:

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

a) **National Hotlines**: Many countries have national hotlines or helplines specifically dedicated to reporting human trafficking, including cyber trafficking. These hotlines are often staffed by trained professionals who can provide assistance and guidance.

The hotline can be reached:

- By phone: 1-888-373-7888
- By email: help@humantraffickinghotline.org
- By text: text HELP to 233733 (BEFREE)
- Online chat: www.humantraffickinghotline.org

Hotline staff are trained to:

- Listen to survivors of all forms of human trafficking
- Provide immediate safety planning for people in crisis
- Field tips of suspected trafficking
- Help survivors understand their options for support without judgment

b) Child abuse hotlines:

CHILDLINE is a National, 24 Hour, Emergency toll free phone service for children in need of care and protection. Any child or concerned adult can dial 1098 to access this service. It is project of The Ministry of Woman and Child Development, Government of India (GOI).

c) Cyber crime portal:

Filing a Complaint on National Cyber Crime Reporting Portal

https://cybercrime.gov.in/Webform/crmcondi.aspx

This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. National women helpline number is 181 and Cyber Crime Helpline is 1930.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

UNIT V

INTERNET ADDICTION AND MANAGEMENT

Meaning –History and Origin of Internet Addiction - Types of Internet Addiction – Risk Factors involved in Addition – Internet Addiction Disorder: Causes, Warning Signs, Symptoms.

Diagnosis – Management: Treatment, Counselling, Support, Computerized Psychotherapy – Tips to Modify Internet Usage.

MEANING

- **Internet addiction disorder** (**IAD**) can otherwise be referred to as **problematic internet use** or **pathological internet use**.
- It is generally defined as problematic, compulsive use of the internet, that results in significant impairment in an individual's function in various aspects of life over a prolonged period of time.
- Young people are at particular risk of developing internet addiction disorder.
- Excessive Internet use has not been recognized as a disorder by the World Health Organization, the Diagnostic and Statistical Manual of Mental Disorders (DSM-5) or the International Classification of Diseases (ICD-11).

HISTORY AND ORIGIN OF INTERNET ADDICTION

- The **Internet evolved from early 1980s** to the modern day revolutionizing the broadcasting, information sharing and connecting individuals worldwide. Today, it has become an in-built part of daily lives of people including children and adolescents.
- There is growing concern about the addictive quality of the Internet, and pioneering researchers have **introduced the concept of addiction (IA) in mid-1990s**
- **IA was introduced as a disorder by Young in her seminal paper "Internet Addiction: The emergence of a new clinical disorder" in 1996.** She proposed diagnostic criteria for IA based on the existing Diagnostic and Statistical Manual of Mental Disorders 4th edition (DSM-4) criteria for substance dependence.
- In **1999, David Greenfield too proposed IA** to be a form of addictive disorder
- Dr. Ivan K. Goldberg, who first broached the concept of Internet addiction, adopted a few criteria for IAD on the basis of DSM-IV
- An increasing incidence of IA together with its high cooccurrence with other established psychiatric disorders was pointed out later . **The proposal to include "Internet addiction disorder" in the 5th edition of Diagnostic and Statistical Manual of Mental Disorders (DSM-5)** was brought forward.
- Lack of consensus on a definition for IA, which is even blurred subcategory of Internet use (i.e., gaming, social media, cybersex, etc.), makes it difficult to derive prevalence data.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

- The world where Internet gaming has an apparent high prevalence, relevant governments such as Chinese have accepted Internet gaming as an established "addiction" and South Korea have identified IA as a problem at governmental level and declared it a serious public health hazard
- The IA as pattern of International Classification of Disease added in 10th version (ICD 10) by World Health Organization (WHO).
- Now Mental healthcare professionals in many countries particularly in Asia and Europe are increasingly urging the authorities such as World Health Organization to identify IA as an independent disorder

TYPES OF INTERNET ADDICTION

a) Problem gambling (online gambling disorder)

- Online gambling is considered to be as serious as pathological gambling.
- It is known as an "isolated disorder" which means that those who have a gambling problem prefer to separate themselves from interruptions and distractions.

b) Internet gaming disorder

- Gaming disorder (colloquially video game addiction) is a known issue and severity grew in the 2000s, with the advent of broadband technology, games allowing for the creation of avatars, 'second life' games, and MMORPGs (massive multiplayer online role playing games).
- *Online gaming addiction may be considered in terms of B.F. Skinner's theory of operant conditioning, which claims that the frequency of a given behaviour is directly linked to rewarding and punishment* of that behavior.
- If a behavior is rewarded, it is more likely to be repeated. If it is punished, it becomes suppressed.

c) Compulsive sexual behaviour disorder (problematic Internet pornography use)

- Pornography addiction is often defined operationally by the frequency of pornography viewing and negative consequences.
- A study on problematic Internet pornography viewing used the criteria of viewing Internet pornography more than three times a week during some weeks, and viewing causing difficulty in general life functioning.

d) Compulsive talking (communication addiction disorder)

- Communication addiction disorder (CAD) is a supposed behavioral disorder related to the necessity of being in constant communication with other people, even when there is no practical necessity for such communication. CAD has been linked to Internet addiction.
- Users become addicted to the social elements of the Internet, such as Facebook and YouTube.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

- Users become addicted to one-on-one or group communication in the form of social support, relationships, and entertainment
- Social network addiction is a dependence of people by connection, updating, and control of their and their friend's social network page.
- For some people, in fact, the only important thing is to have a lot of friends in the network regardless if they are offline or only virtual.
- Sometimes teenagers use social networks to show their idealized image to the others.[

e) Compulsive VR use

- Compulsive VR use (colloquially virtual-reality addiction) is a compulsion to use virtual reality or virtual, immersive environments. Currently, interactive virtual media (such as social networks) are referred to as virtual reality.

f) Video streaming addiction

- Video streaming addiction is an addiction to watching online video content, such as those accessed through free online video sharing sites such as YouTube, subscription streaming services such as Netflix, as well as livestreaming sites such as Twitch.
- On positive note, the social nature of the internet has a reinforcing effect and replaced on the individual's binge-eating behaviour while watching television series.

g) Wikipedia addiction

- As of 2016, addiction to Wikipedia has been documented in psychiatry journals.

RISK FACTORS INVOLVED IN ADDITION

Interpersonal difficulties

Internet-based relationships offer a safe alternatives for those who have interpersonal difficulties such as introversion, social problems, and poor face-to-face communication skills to escape from the potential live rejections and anxieties of real-life contact.

Social support

Individuals who lack sufficient social connection and social support are found to run a higher risk of Internet addiction. They resort to virtual relationships and support to escape their loneliness.

As a matter of fact, the most prevalent applications among these Internet addicts are

- ✓ chat rooms,
- ✓ interactive games,

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

- ✓ instant messaging, or social media

Some empirical studies reveal that conflict between parents and children and not living with mother are at high risk to be significantly associated with IA

Psychological factors

- ❖ Some individuals with prior psychiatric problems such as depression and anxiety turn to compulsive behaviors to avoid the unpleasant emotions and situation of their psychiatric problems and regard being addicted to the Internet a safer alternative to substance addictive tendency.
- ❖ The most common co-morbidities that have been linked to IAD are major depression and attention deficit hyperactivity disorder (ADHD).

Internet addicts with no previous significant addictive or psychiatric history are argued to develop an addiction due to some features of Internet use such as

- ✓ anonymity,
- ✓ easy accessibility, and
- ✓ its interactive nature.

Neurobiological factors

- ❖ One of the main challenges in the development of the bio-psychosocial model of Internet addiction is to *determine which genes and neuro mediators are responsible for increased addiction susceptibility*.
- ❖ Internet addiction belongs to the group of multifactorial polygenic disorders. For each specific case, there is a *unique combination of inherited characteristics (nervous tissue structure, secretion, degradation, and reception of neuromediators), and many are extra-environment factors (family-related, social, and ethnic-cultural) as reason for neurobiological problems*.
- ❖ Internet Gamind Disorder(*IGD) is associated with alterations in brain regions involved in reward processing, impulse control, decision-making, and executive functioning*. These changes in neural activity may result in the persistent and excessive use of internet gaming and may contribute to the development of IGD.

Other factors

- ❖ Parental educational level,
- ❖ age at first use of the Internet, and
- ❖ the frequency of using social networking sites and gaming sites are found to be positively associated with excessive Internet use among adolescents.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

INTERNET ADDICTION DISORDER: CAUSES, WARNING SIGNS, SYMPTOMS

- Internet addiction refers to the compulsive need to spend a great deal of time on the Internet, to the point where relationships, work and health are allowed to suffer.

CAUSES OF IAD

- Internet use triggers **a sense of reward** in the brain that leads to more use.
- Whenever **Internet addicts feel overwhelmed, stressed, depressed, lonely or anxious**, they use the Internet to seek peace and escape.
- Studies from the University of Iowa show that Internet addiction is quite common among males ages 20 to 30 years old who are **suffering from anxiety and depression**.
- There are also those who have a **history of other types of addiction, such as addictions to alcohol, drugs, sex and gambling.**
- Even being **stressed and unhappy** can contribute greatly to the development of a computer or Internet addiction.
- People who are **overly shy and cannot easily develop interpersonal relationship, introverts** are also at a higher risk of developing a computer or Internet addiction.

Other risk factors are:

- ✓ Being male.
- ✓ Having a mental health condition.
- ✓ Having poor moods.
- ✓ Having limited offline social time.
- ✓ Family conflict.

WARNING SIGNS & SYMPTOMS OF IAD

PHYSICAL SYMPTOMS	PSYCHOLOGICAL SYMPTOMS	SOCIAL SYSMPTOMS
Physical symptoms include a weakened immune system due to lack of sleep, • loss of exercise, and increased risk for carpal tunnel syndrome and • eye and back strain	• Feelings of guilt • Anxiety • Depression • Dishonesty • Euphoric feelings when in front of the computer • Unable to keep schedules • No sense of time	• Isolation • Strained interpersonal relationship

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

• Changes in physical appearance • Digestive problem • Weight gain or loss • Stiff limbs • Bad posture • Shoulder pain	• Isolation • Defensiveness • Avoiding doing work • Agitation	

DIAGNOSIS OF IAD

Diagnosis of Internet addiction disorder is empirically difficult. Various screening instruments have been employed to detect Internet addiction disorder. Current diagnoses are faced with multiple obstacles.

I. DSM-based instruments

Dr. Kimberly S. Young (1998) proposed one of the first integrated sets of criteria, *Diagnostic Questionnaire (YDQ),* to detect Internet addiction. A person who fulfills any five of the eight adapted criteria would be regarded as Internet addicted:

1. Preoccupation with the Internet;
2. A need for increased time spent online to achieve the same amount of satisfaction;
3. Repeated efforts to curtail Internet use;
4. Irritability, depression, or mood lability when Internet use is limited;
5. Staying online longer than anticipated;
6. Putting a job or relationship in jeopardy to use the Internet;
7. Lying to others about how much time is spent online; and
8. Using the Internet as a means of regulating mood.

Dr. Kimberly S. Young (1999) says that IAD leads to several subtypes of behavior and impulse control problems, namely

- ❖ Cybersexual addiction: compulsive use of adult websites for cybersex and cyberporn (see Internet sex addiction)
- ❖ Cyber-relationship addiction: Over-involvement in online relationships
- ❖ Net compulsions: Obsessive online gambling, shopping or day-trading
- ❖ Information overload: Compulsive web surfing or database searches
- ❖ Computer addiction: Obsessive computer game playing (see Video game addiction)

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

II. Oher instruments

Over time, a considerable number of screening instruments have been developed to diagnose Internet addiction, including the

- Internet Addiction Test (IAT),
- Internet-Related Addictive Behavior Inventory (IRABI),
- Chinese Internet Addiction Inventory (CIAI),
- Korean Internet Addiction Self-Assessment Scale (KS Scale)
- Compulsive Internet Use Scale (CIUS)
- Generalized Problematic Internet Use Scale (GPIUS),
- Internet Consequences Scale (ICONS), and

Problematic Internet Use Scale (PIUS).

The Internet Addiction Test (IAT) by Young (1998) exhibits good internal reliability and validity and has been used and validated worldwide as a screening instrument.

III. Single-question instruments

Some scholars and practitioners also attempt to define Internet addiction by a single question, typically the time-use of the Internet

IV. Neuroimaging techniques

Emergent neuroscience studies investigated the influence of problematic, compulsive use of the internet on the human brain. neuroimaging studies revealed that IAD contributes to structural and functional abnormalities in the human brain, similar to other behavioral and substance additions.

V. Electroencephalography-based diagnosis

Using electroencephalography (EEG) readings allows identifying abnormalities in the electrical activity of the human brain caused by IAD. Studies revealed that individuals with IAD predominantly demonstrate increased activity in the theta and gamma band and decreased delta, alpha, and beta activity.

MANAGEMENT OF IAD

- The new technology evolves and societies have to keep abreast with the development for successful survival. Therefore, total banning of an adolescent from using the Internet is not the answer.
- In other words, total abstinence should not be the goal.
- Instead, controlled/safe/balanced or more preferably sensible Internet usage should be the goal.

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

- Both the treating clinician and the affected individual should come to a consensus about the details of **sensible use** depending on the age, educational demands, cultural value system, etc.

TREATMENT OF IAD

Current interventions and strategies used as treatments for Internet addiction stem from those practiced in substance abuse disorder. Psychosocial treatment is the approach most often applied. In practice, rehab centres usually devise a combination of multiple therapies.

1. PSYCHOSOCIAL TREATMENT

Cognitive Behavioural Therapy

The cognitive behavioral therapy with Internet addicts (CBT-IA) is developed in analogy to therapies for impulse control disorder.

Several key aspects are embedded in this therapy:

- Learning time management strategies;
- Recognizing the benefits and potential harms of the Internet;
- Increasing self-awareness and awareness of others and one's surroundings;
- Identifying "triggers" of Internet "binge behavior", such as particular Internet applications, emotional states, maladaptive cognitions, and life events;
- Learning to manage emotions and control impulses related to accessing the Internet, such as muscles or breathing relaxation training;
- Improving interpersonal communication and interaction skills;
- Improving coping styles;
- Cultivating interests in alternative activities.

Three phases are implemented in the CBT-IA therapy:

1. **Behavior modification to control Internet use:** Examine both computer behavior and non-computer behavior and manage Internet addicts' time online and offline;
2. **Cognitive restructuring to challenge and modify cognitive distortions**: Identify, challenge, and modify the rationalizations that justify excessive Internet use;
3. **Harm reduction therapy to address co-morbid issues**: Address any co-morbid factors associated with Internet addiction, sustain recovery, and prevent relapse.

Symptom management of CBT-IA treatment has been found to sustain six months post-treatment

2. MOTIVATIONAL INTERVIEWING (COUNSELLING SUPPORT)

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

The motivational interviewing approach is developed based on therapies for alcohol abusers.

This therapy is a directive, patient-centered counseling style for eliciting behavior change through helping patients explore and resolve ambivalence with a respectful therapeutic manner.

It does not, however, provide patients with solutions or problem solving until patients' decision to change behaviors

Several key elements are embedded in this therapy:

- ✓ Asking open-ended questions;
- ✓ Giving affirmations;
- ✓ Reflective listening

Other psychosocial treatment therapies include

- ✓ Reality therapy,
- ✓ Naikan cognitive psychotherapy,
- ✓ Group therapy,
- ✓ Family therapy, and
- ✓ Multimodal psychotherapy

3. PHARMACOLOGUICAL TREATMENT

The antidepressants that have been most successful are selective serotonin reuptake inhibitors (SSRIs) such as

- ✓ escitalopram and the
- ✓ atypical antidepressant bupropion.
- ✓ A psychostimulant,
- ✓ methylphenidate, was also found to have beneficial effects

4. COMPUTERISED PSYCHOTHERAPY

Computerized Psychotherapy uses software to administer dynamic mental health interventions with no (or limited) therapist involvement.

Computerized psychotherapy can take many forms, including

- ✓ stand-alone programs,
- ✓ virtual reality programs,
- ✓ cognitive bias modification, and

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

- ✓ different types of internet-delivered psychotherapy.

Of these, internet-based cognitive behavioral therapy (ICBT) is the most well-investigated format.

However, forms of therapy that rely more heavily on verbal interaction and the patient-therapist relationship are not yet possible.

5. VIRTUAL REALITY THERAPY

Virtual reality (VR) places people in a simulated and imaginary environment, typically through the use of a stereoscopic headset. VR has the advantage that the system designers have complete control over what the user sees and hears.

TIPS TO MODIFY INTERNET USAGE.

The following are some simple techniques based on behavior therapy with or without cognitive component that can be utilized to use the Internet sensibly

a) Admit it

The first step to solve any sort of problem is to step out of the denial phase and accept that you have a problem

b) Healthy digital nutrition and modelling by adults

Having a prior discussion and an agreement on Internet use before a family purchase Internet facility. All in the household following through the plan.

c) Disconnect to reconnect

Setting aside devices at family/friends gatherings and meal times.

d) Digital Detox

Get set to lit smartphone usage.

Having a family Internet-free day probably on a Sunday so that education or work/business is not affected.

e) Keep devices inaccesible

When at studies or assignments switching of the notifications of chat sites or social networks just the way people place mobile phones on silent mode or switch them off.

f) Allocation of time for socializing

Have an assigned time for socializing on the net (by using an alarm) and setting limits on checking on social media responses, for example, only three times per day or once a week. (

g) Doing it real

Mrs.Aarthi. D, M.A., M.Phil
Assistant Professor and Head
Department of Psychology
DKM College for Women (Autonomous)

Internet times to be replaced by more attractive offline activities (not offline studies!) such as getting together with friends in real life, competitive or recreational sports, aerobics, etc. (Doing it in real)

h) Rewarding

Reward for being off Internet as planned, for example, by having a vacation every 3 months or weekend movie/dinner out.