XXXXXXXXXX

SUBMITTED TO-

XXXXXXXXXXX

CYBER ETHICS

SCRAP FILE

CLASS-

XXXXXXXXX

XXXXXXX

SUBMITTED BY-

XXXXXXXX

INDEX

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to my teacher as well who gave me the golden opportunity to do this wonderful project on the topic (Cyber Ethics), which also helped me in doing a lot of Research and i came to know about so many new things. I am really thankful to them.

INTRODUCTION TO CYBER ETHICS

Cyber ethics is the study of ethics pertaining to computers, covering user behavior and what computers are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while organizations have explained policies about cyber ethics.

With the increase of young children using the internet, it is now very essential than ever to tell children about how to properly operate the internet and its dangers.

FOUNDATION OF CYBER ETHICS-

Computer ethics was first coined by Walter Maner, a professor at Bowling Green State University. Maner noticed ethical concerns that were brought up during his Medical Ethics course at Old Dominion University became more complex and difficult when the use of technology and computers became involved. The conceptual foundations of computer ethics are investigated by information ethics, a branch of philosophical ethics promoted, among others, by Luciano Floridi.

HISTORY OF CYBER ETHICS

The concept of computer ethics originated in the 1940s with MIT professor Nobert Wiener, the American mathematician and philosopher. While working on anti-aircraft artillery during World War II, Wiener and his fellow engineers developed a system of communication between the part of a cannon that tracked a warplane, the part that performed calculations to estimate a trajectory, and the part responsible for firing. Wiener termed the science of such information feedback systems, "cybernetics", and he discussed this new field with its related ethical concerns in his 1948 book, *Cybernetics*.

IMPORTANCE OF CYBER ETHICS

- To protect personal & commercial information such as login & password info, credit card and account information and government and commercial databases. It also controls unwanted internet mail and ads (Spam).
- To control plagiarism, student identity fraud, and the use of copyrighted material, etc.
- To make ICT available and accessible to all peoples, including the disabled and the deprived. Accessibility needs to be kept in mind during curriculum design (in educational contexts), in order to maximize the capabilities of the technology
- To suppress dishonest business practices and to protect and encourage fair competition
- To promote moral and social values in society

RULES OF CYBER ETHICS

•Do not break into someone else's computer.Do not cyberbully.

Do not plagiarize

Do not cyberbully.

•Do not break into someone else's computer.

•Do not use rude or offensive language Adhere to copyright restrictions

•Do not attempt to infect or in any way try to make someone else's computer unusable.

RESPONSIBLE BEHAVIORS ON THE INTERNET

Cyber ethics concerns to the code of responsible behavior on the Internet. Just as we are taught to act responsibly in everyday life. The responsible behavior on the internet in many ways aligns with all the right behavior in everyday life, but the results can be significantly different.

Some people try to hide behind a false sense of obscurity on the internet, believing that it does not matter if they behave badly online because no one knows who they are or how to search them. That is not all the time true; browsers, computers and internet service providers may keep logs of their activities which can be used to spot illegal or inappropriate behavior.

The Government has taken a positive role in making resources for parents and children to learn about cyber ethics. This is a growing problem and without parents and teachers using the resources available nothing can be done to prepare future generations of internet users from being safe online.

CRIME AND PUNISHMENT

Children do not believe that they will get into any real problem from neglecting the use of cyber ethics. It has become easy to track the origin of wrong activity over the internet to an individual user. There is not much anonymity as a child may trust. The United States Department of Justice has a recent list of Federal Computer Crime Cases teens this is a best way to show children the costly consequences of their internet actions.

Crime and punishment in cyber world

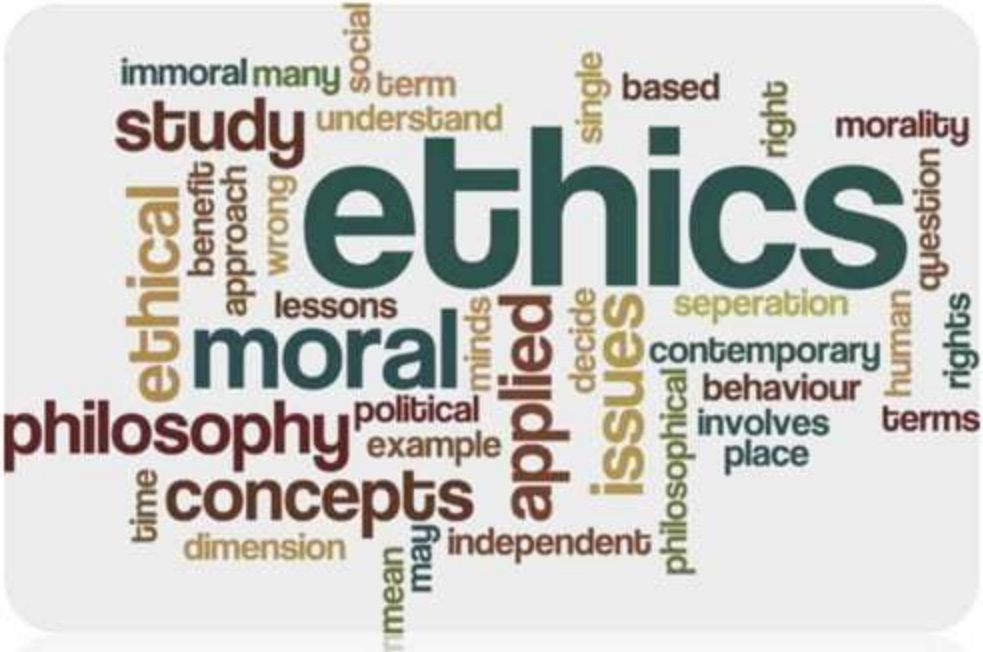
The author explores the legal position on key topics of internet and digital communications

CYBER ETHICS RELEVANCE IN TODAY'S WORLD

- To protect personal & commercial information such as login & password info, credit card and account information and government and commercial databases. It also controls unwanted internet mail and ads (Spam).
- To control plagiarism, student identity fraud, and the use of copyrighted material, etc.
- To make ICT available and accessible to all peoples, including the disabled and the deprived. Accessibility needs to be kept in mind during curriculum design (in

educational contexts), in order to maximize the capabilities of the technology

- To suppress dishonest business practices and to protect and encourage fair competition
- To promote moral and social values in society



Following some issues are increasing daily due to children using the internet improperly and we have to take care of it.

EXAMPLES:

I. COPYRIGHTING OR DOWLOADING

Copyright or downloading is a major issue because children don't know copyright policies. They only try to search what they need from the web and download it for their purpose. Their thinking is like "if everybody is doing it therefore it's ok", but an understandable and an age appropriate lesson on Cyber Ethics could help children to learn the risks involved in Internet downloading.

II. CRIME AND PUNISHMENT

Children do not believe that they will get into any real problem from neglecting the

use of cyber ethics. It has become easy to track the origin of wrong activity over the internet to an individual user. There is not much anonymity as a child may trust. The United States Department of Justice has a recent list of Federal Computer Crime Cases teens this is a best way to show children the costly consequences of their internet actions.

III. INTERNET HACKING

Hacking done by stealing classified information, stealing passwords to get into a site and also recasting a website without permission. Since the world is run on computers it is important that hackers are stopped. They could create viruses that could shut down important websites or computer systems. So we have to make our children aware by telling its importance.

IV. CYBERBULLYING

Hacking done by stealing classified information, stealing passwords to get into a site and also recasting a website without permission. Since the world is run on computers it is important that hackers are stopped. They could create viruses that could shut down important websites or computer systems. So we have to make our children aware by telling its importance.

When a child encounters cyber bullying that they should:

- Tell a trusted adult, and keep telling them until they take action.
- Avoid to open, read or respond to messages from cyber bullies.
- Always keep messages from bullies. They may be needed to take corrective action
- Use software to block bullies if they encounter them through chat or IM.

FIVE PROVISIONS OF CYBER ETHICS

- Your computer or system should not be used to harm others.
- Your cyber knowledge should not be used to steal other people's resources.
- One should not use or copy softwares for which you have not paid.
- You should not break into someone else's accounts.

- Never use other people's resources without their consent.

DO'S AND DON'T IN CYBER ETHICS

	DO	DON'T
Schoolwork	Use the internet to help you do the homework. You can find many information inside the internet.	Don't copy other people works and call it your own. Do credits to the author or website.
Music, videos and copyright	Use the internet to learn about music, video and games.	Don't use the internet to download or share copyrighted material.

	DO	DON'T
E-mail and instant messaging (IM)	Use the internet to communicate with friends and family. But make sure you know to whom you exchange your e-mail and IM	Don't use the internet to communicate with strangers. Don't pretend to be someone else and don't be rude or use bad language.
For Parents	Encourage your children to use the Internet. The Internet has a lot good things to offer children.	Don't leave your children unsupervised. Make sure you know what sites your children visit when they're on the internet, and with whom they're communicating. Look over their shoulder. Keep track of the

BASIC QUESTIONS RELATED TO CYBER ETHICS-

- **Why do we teach CYBER ETHICS ?**

There are 5 convincing teaching cyber ethics is a must in today's environment :

1. **Increasingly Accessible Smart Devices**

it has become increasingly more likely for children to receive their first smart device at an early age.

Before we delve into doom and gloom, it's vital to understand that cellphones are useful tools, especially for single children. School may finish sooner than expected, or they might want to sleepover at a friends' birthday party and get in touch with home quickly. The problem rears its head when we add social media platforms with unrestricted access to various types of content into the equation. Parents who take a proactive approach to issues and explain cyberethics of right and wrong uses of smart devices are doing the right thing. It's inevitable that a young child will come across video ads or photos which don't correspond with their age – be proactive and explain cyberethics.

2. Address Cyber Myths & Common Threats

While some cyber threats fall squarely into prejudices, others are very real and pose a serious threat to young children. For example, phishing scams which aim to collect credit card or ID information from devices are real but can be avoided through careful device use. Banner ads which offer free games or coupons if a child clicks on them, however, almost always contain harmful malware. These threats may seem arbitrary to an adult or a millennial that grew up as they became known to the public. However, young children have no prior experience with harmful content, which aims to steal their data or make their device defective. Take the time to explain these concepts to your student group or child, and they are very likely to become more careful in the future.

3. Explain the Context of Cyber Communication

Social media platforms and instant messaging apps are amazing tools which can help connect children with their peers across the globe. They also open the door for cyberbullying, identity theft, and other fraudulent behavior, which can harm the mental well-being of your child.To

avoid this, make it a habit to use these platforms with your child and explain to them the meaning of online textual communication. Emphasize that the words and statements they type and send to friends mean as much as real words spoken out loud. If they tell a friend a bad word, that word will sting and hurt their relationship as much as a real fight would. Children often lack the perspective to understand online communication, and teaching them about it is an integral part of cyberethics

4. Learning How to Stay Safe in Cyberspace

Ransomware, malware, Trojan viruses, and malicious software can be extremely easy to download onto a laptop or smart device. Based on 99 Firms, cyber-attacks happen 2,244 times per day, with 71% being financially motivated and 64% of Americans never checking if they were attacked. It's essential that children know the difference between legitimate software and online content and that which can harm them.Likewise, many online platforms request private information or access to smart device's camera, phonebook, and other data unrelated to their functionality. In the case of K-12 students, parents should make it a habit to check on their children's device, set parental controls, and help

ensure their safety. While micromanagement of security parameters may seem counterintuitive in regards to parenting, this is the only way to secure a child's smart device.

5. Copyright & Content Authorship Explanation

As children move closer to high school, they are bound to start posting their original content on the web. Platforms such as Tumblr are a perfect playground for children to stretch their creative muscles and develop new competencies. However, this opens the door for copyright, authorship, and ownership issues in case of fan art or republished content. Companies such as Disney and Nintendo are not very keen on letting others post their content under a different name.To avoid legal issues and to help children understand the context of online ownership, you should encourage them to create original content instead. Start by introducing the concept of Creative Commons and how they can protect their original creations from copyright abuse. Later, platforms like Evernote or a research paper writing service, in addition to visual-based platforms like Canva, can help your child develop creative skills. Content created through these and similar services will be original and allow

children to share, edit, and republish their creations as much as possible.

- **What is the need for Cyber Ethics?**

The need to behave in a morally accountable manner in the cyber-domain — on social media sites, in email communications, on bank websites, and so forth — then it seems to me an unproblematical question to answer; in the affirmative, that is. This is one of the major sources of ethical/moral transgressions, or arguably even more seriously, of cyber-crime, in virtual space, and assumes the form of hacking into people's bank accounts and stealing their money, or defrauding people in a myriad of ways, some more direct than others. Such behaviour may occur in cyber-space, but it is in principle no different from robbing a person at gunpoint. There are many kinds of ethically or morally reprehensible behaviour, and of cyber-

crime, in the space opened up by the internet — from actions involving people's financial status, through hate-speech or — writing regarding gender, race, culture, and a host of other morally dubious (if not constitutionally illegal) actions such as governments or corporations spying on individuals, individuals spying on governments or corporations, and so on. But this is not the only meaning of "the need for cyber-ethics" — the obligation to act ethically towards others, just as one is implicitly expected to do so in ordinary, everyday social space; an obligation that is impossible to enforce, by the way, as we all know. The most one can expect is that other people will follow the "live ethically and expect others to do the same" principle.

5 COMMON ETHICAL ISSUES IN WORKPLACE

Recent headline-making ethical issues, particularly those tied to discrimination and sexual harassment, have shed light on unethical conduct in the workplace and how these ethical lapses can permeate employee relations, business practices, and operations. According to the **Ethics & Compliance Initiative's 2018 Global Benchmark on Workplace Ethics**, 30% of employees in the U.S. personally observed misconduct in the past 12 months, a number close to the global median for misconduct observation. These ethical breaches often occur unreported or unaddressed, and when totaled, can command a hefty cost. Unethical practices spurred more than half of the largest bankruptcies in the past 30 years, like Enron, Lehman Brothers, and WorldCom, and can take a larger economic toll, estimated at $1.228 trillion, according to the **Society for Human Resource Management**.

UNETHICAL LEADERSHIP-

Having a personal issue with your boss is one thing, but reporting to a person who is behaving unethically is another. This may come in an obvious form, like manipulating numbers in a report or spending company money on inappropriate activities; however, it can also occur more subtly, in the form of bullying, accepting inappropriate gifts from suppliers, or asking you to skip a standard procedure *just once*. With studies indicating that managers are responsible for **60% of workplace misconduct**, the abuse of leadership authority is an unfortunate reality.

TOXIC WORKPLACE CULTURE-

Organizations helmed by unethical leadership are more often than not plagued by a toxic workplace culture. Leaders who think nothing of taking bribes, manipulating sales figures and

data or pressuring employees or business associates for "favors" (whether they be personal or financial), will think nothing of disrespecting and bullying their employees. With the current emphasis in many organizations to hire for "cultural fit," a toxic culture can be exacerbated by continually repopulating the company with like-minded personalities and toxic mentalities. Even worse, hiring for "cultural fit" can become a smokescreen for discrimination, which can result in more ethical issues and legal ramifications.

DISCRIMINATION AND HARASSMENT-

Laws require organizations to be equal employment opportunity employers. Organizations must recruit a diverse workforce, enforce policies and training that support an **equal opportunity program**, and foster an environment that is respectful of all types of people. Unfortunately, there are still many whose

practices break with EEOC guidelines. When discrimination and harassment of employees based on race, ethnicity, gender, disability or age occurs, not only has an ethical line been crossed but a legal one as well. Most companies are vigilant to avoid the costly legal and public ramifications of discrimination and harassment, so you may encounter this ethical dilemma in more subtle ways, from seemingly "harmless" off-color jokes by a manager to a more pervasive "group think" mentality that can be a symptom of a toxic culture. This could be a group mentality toward an "other" group (for example, women aren't a good fit for our group). Your best response is to maintain your personal values and repel such intolerant, unethical or illegal group norms by offering an alternative, inclusive perspective as the best choice for the group and the organization.

UNREALISTIC AND CONFLICTING GOALS-

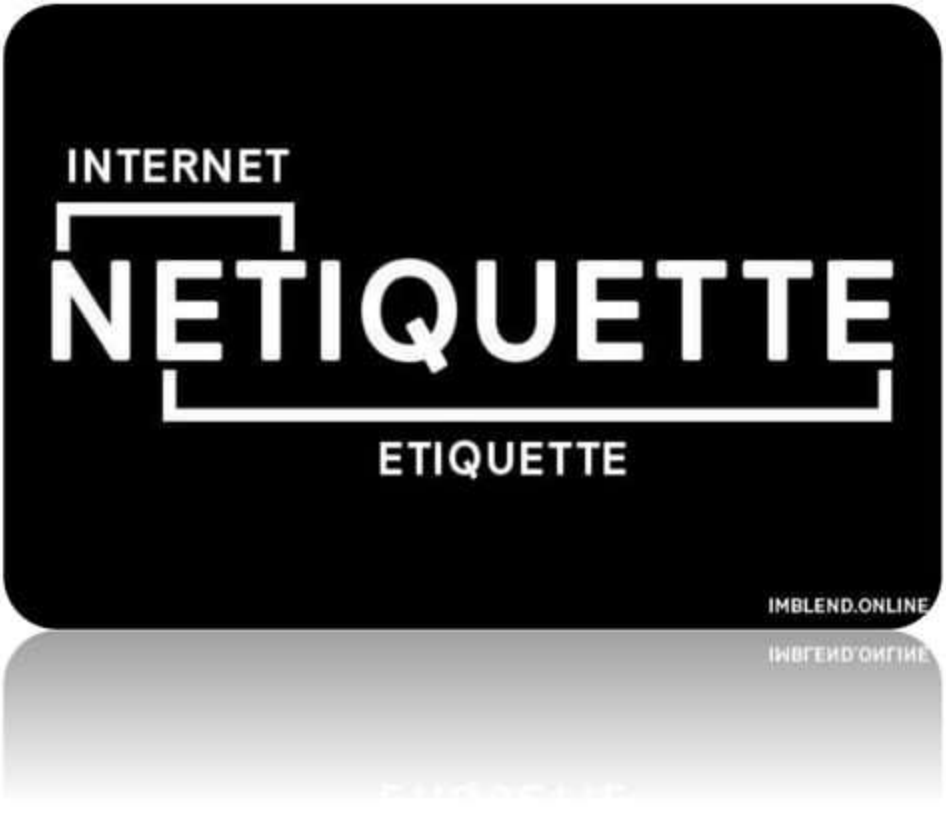
Your organization sets a goal—it could be a monthly sales figure or product production number—that seems unrealistic, even unattainable. While not unethical in and of itself (after all, having driven leadership with aggressive company goals is crucial to innovation and growth), it's how employees, and even some leaders, go about reaching the goal that could raise an ethical red flag. Unrealistic objectives can spur leaders to put undue pressure on their employees, and employees may consider cutting corners or breaching ethical or legal guidelines to obtain them. Cutting corners ethically is a shortcut that rarely pays off, and if your entire team or department is failing to meet goals, company leadership needs that feedback to revisit those goals and re-evaluate performance expectations.

QUESTIONABLE USE OF COMPANY TECHNOLOGY-

While this may feel like a minor blip in the grand scheme of workplace ethics, the improper use of the internet and company technology is a huge cost for organizations in lost time, worker productivity and company dollars. One survey found that **64% of employees** visit non-work related websites during the workday. Not only is it a misuse of company tools and technology, but it's also a misuse of company time. Whether you're taking hourly breaks to check your social media news feed or know that your coworker is using company technology resources to work on freelance jobs, this "little white lie" of workplace ethics can create a snowball effect. The response to this one is simple: when you're working on the company's computer on the company's time, just don't do it, even as tempting as it may be.

NETIQUETTE

Netiquette is a combination of the words network and etiquette and is defined as a set of rules for acceptable online behavior. Similarly, online ethics focuses on the acceptable use of online resources in an online social environment.



Both phrases are frequently interchanged and are often combined with the concept of a 'netizen' which itself is a contraction of the words internet and citizen and refers to both a person who uses the internet to participate in society, and an individual who has accepted the responsibility of using the internet in productive and socially responsible ways.

NETIQUETTE GUIDELINES-

- **Be friendly, positive and self-reflective.** When people cannot see you, and also do not know you, feelings can be hurt if you are not careful in how you express yourself. The old saying, think before you speak is important here. Think before you write. One word of advice is do not respond when you feel angry. Wait. Write it down somewhere and come back to it. When you do, you may find that you no longer feel the same way as you did when you wrote it, because you have had time to reflect about the situation.
- **Use proper language and titles.** Do not use slang or even profane words in an online environment, even if they are words you consider, "not so bad," as they will sound offensive to the reader. Do not refer to your professor as "Doc" or by his or her first name, unless it is acceptable with him or her to do so. Also, do not use caps lock when writing. It will insinuate yelling. That would hurt someone's feelings and possibly give him or her the wrong impression of you.
- **Use effective communication.** This takes practice and thoughtful writing. Try to speak and write clearly at all times. Again, reread before you respond. Define and restate your words when necessary. Correct a misunderstanding right away. Chances are, if one person felt a certain way about what you said, then another may have as well. Likewise, be mindful of chosen words and joking. Let's say for example, I write, "get out!" This slang term can be interpreted in several ways, either positively or negatively.

- **Professionalism.** Leave the characters like smiley faces, and instant message abbreviations out. Your friends may like it, but chances are, your professor will not. Save it for personal conversations or definitely ask for permission before using them. They may be interpreted as childish or too casual for the online education environment. Last, always say please and thank you.

- **Ask for clarification.** If you are unsure of what was said, or the instructor's directive, or are trying to interpret a person's expressions, then ask again. Do not sit in silence either misunderstanding or feeling offended. Do not interrupt though, wait until there is a break in the conversation, or until the open interaction occurs. Your instructor will appreciate your responsiveness and maturity. A simple way to do this is to say (or write), "I did not understand...", always keeping the onus for the misunderstanding on yourself. With these top five netiquette rules, you are on your way to online success!

RULES OF NETIQUETTE AND AREAS OF COMPUTER ETHICS-

RULES-

- Netiquette, or net etiquette, refers to etiquette on the Internet.
  Is the code of acceptable behaviours users should follow while on the Internet or online or cyberspace.
- It is the conduct expected of individuals while online.
  - Rules for all aspects of the:
    - World Wide Web
    - E-mail
    - Instant Messaging
    - Chat rooms
    - Newsgroups & message board.

When do these rules apply?

- Chatting online
- Using email
- Posting to a discussion
- Blogging
- Playing online games
- Social media
- Using web
- Internet messagin

Netiquette Guidelines for Online Communications

Golden Rule: Treat others as you would like them to treat you.

Be polite. Avoid offensive language.

Avoid sending or posting *flames*, which are abusive or insulting messages. Do not participate in *flame wars*, which are exchanges of flames.

Be careful when using sarcasm and humor, as it might be misinterpreted.

Do not use all capital letters, which is the equivalent of SHOUTING!

Use **emoticons** to express emotion. Popular emoticons include:

:) Smile :| Indifference :o Surprised :(Frown :\ Undecided ;) Wink

Use abbreviations and acronyms for phrases:

BTW	by the way	IMHO	in my humble opinion	FWIW	for what it's worth
FYI	for your information	TTFN	ta ta for now	TYVM	thank you very much

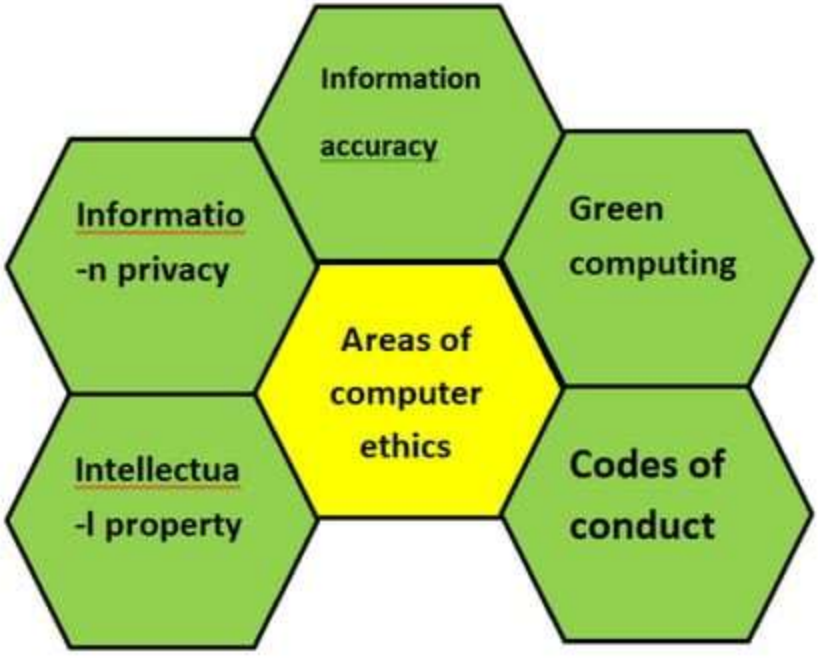
Clearly identify a spoiler, which is a message that reveals an outcome to a game or ending to a movie or program.

Be forgiving of other's mistakes.

Read the *FAQ* (frequently asked questions), if one exists.

AREAS OF COMPUTER ETHICS

The moral guidelines that govern the use of computers, mobile devices and information systems.



INFORMATION ACCURACY

- One of the concern because many users access information maintained by other people or companies, such as on the Internet.
- Do not assume all the information on the Web is correct.
- Users should evaluate the value of a Web page before relying on its content.
- Be aware that the organization providing access to the information may not be the creator of the information.

GREEN COMPUTING

Green computing is the environmentally responsible and eco-friendly use of computers and their resources. In broader terms, it is also defined as the study of designing, manufacturing/engineering, using and disposing of computing devices in a way that reduces their environmental impact.

- Involves reducing the electricity and environmental waste while using a computer.
- Society has become aware of this waste and is taking measures to combat it.
- Some of the actions that has been taken:

i) Using energy- efficient devices that require little power when they are not in use.

ii) Buy computers with low power consumption processors and power supplies.

iii) When possible, use outside air to cool the data center.

- Average computer users can employ the following general tactics to make their computing usage more green:

i) Use the hibernate or sleep mode when away from a computer for extended periods.

ii) Use flat-screen or LCD monitors, instead of conventional cathode ray tube (CRT) monitors.

iii) Buy energy efficient notebook computers, instead of desktop computers.

iv) Activate the power management features for controlling energy consumption.

v) Turn off computers at the end of each day.

vi) Refill printer cartridges, rather than buying new ones.

CODES OF CONDUCT

Written guideline that helps determine whether a specific action is ethical/unethical or allowed/not allowed.

IT Code of Conduct
1. Computers may not be used to harm other people.
2. Employees may not interfere with others' computer work.
3. Employees may not meddle in others' computer files.
4. Computers may not be used to steal.
5. Computers may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' computer resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use computers in a way that demonstrates consideration and respect for fellow humans.

Sample IT code of conduct employers may distribute to employees.

INTELECTUAL PROPERTY

· Unique and original works such as ideas, inventions, literary and artistic works, processes, names and logos.Or, refers to creations of the mind:inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.Intellectual property rights are the rights to which creators are entitled for their work.

i) PATENT

a) A patent is a set of exclusive rights granted by a government to an inventor or applicant for a limited amount of time (normally 20 years from the filing date).

b) It is a legal document defining ownership of a particular area of new technology.

c) Invention - a product or a process that provides a new way of doing something, or offers a new technical solution to a problem.

d) The right granted by a patent excludes all others from making, using, or selling an invention or products made by an invented process.

ii) TRADEMARK

a) Trademark is a word, phrase, symbol, design, combination of letters or numbers, or other device that identifies and distinguishes products and services in the marketplace.

b) Or a distinctive sign which identifies certain goods or services.

c) Or can be any distinctive name or logo.

d) Examples of well-known Trademarks are:

Coca-Cola ,Samsung,The Apple logo ,The Nike "swoosh".

iii) COPYRIGHT

a) Protection provided to the authors of "original works" and includes such things as literary, dramatic, musical, artistic, and certain other intellectual creations, both published and unpublished.

b) Copyright is an exclusive right and gives its creator, or owner :

To reproduce the copyrighted work

To prepare derivative works

To distribute and sell any copies of the copyrighted work

To perform or display the copyrighted work public

RELATED QUESTION-

What Does Good Web Etiquette Look Like?

Underlying this overall concept of socially responsible internet use are a few core pillars, though the details underneath each pillar are still subject to debate.

For Society:

- **Recognizing that the internet is an extension of society.** The internet isn't a new world in which anything goes, but rather, a new dimension of the world around us.
- **Applying the same standards online as we do in public.** In simple terms, this means that the values society has in place against hate speech and bigotry, child exploitation, and child pornography, copyright violations and other forms of theft, remain intact. Values around

courtesy, kindness, openness, and treating others with the same respect we wish to receive should also be adhered to.

- **Refusing to empower abuse and harassment while online.** Accepting that the laws which are currently in place to protect the rights and dignity of citizens apply online and that where needed, laws are updated to reflect these rights in the extended environment. Theft, harassment, and bullying while online is still theft, harassment, and bullying, period.
- **Acknowledging cultural differences.** Even when national boundaries no longer apply, cultural respect and tolerance should remain. This requires finding a way to accept that the social values and norms of some netizens will not be the social values and norms of all netizens.

For Businesses:

For companies, being a good netizen, applying online ethics, and using netiquette include:

- **Respecting rights of privacy for offline employees.** Information possessed by citizens in their offline interactions should be respected.
- **Maintaining transparency in information policies.** By taking action so that consumers can easily and quickly understand how that company is using their information and protecting them from harm, companies can provide users with a clear means of ownership and self-determination as to what is, and isn't shared about them, which strengthens the consumer relationship.

Most internet users automatically apply the same responsible respectful behavior online as they do in every other environment and by nature apply netiquette an online ethics, and are good netizens. The minority that fails to apply societal values in some or any environment- including the internet- are quickly identified as exceptions to be dealt with on a social, or criminal level. When you choose to partner with technology companies,

especially for something as important as internet security, it's imperative you ensure that the partner shares your understanding of what it means to act ethically online.

CYBER CRIME

Cybercrime, also called **computer crime**, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

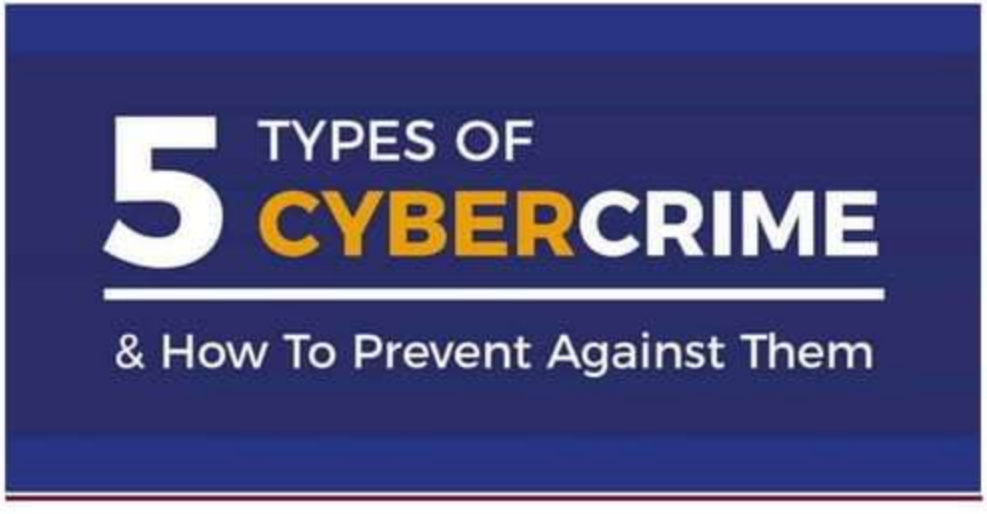
Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

TYPES OF CYBER CRIME-

Different types of cybercrimes have different punishments in India-

- **Identity theft** - When personal information of a person is stolen with the purpose of using their financial resources or to take a loan or credit card in their name then such a crime is known as Identity theft.
- **Cyberterrorism** - When a threat of extortion or any kind of harm is being subjected towards a person, organization, group or state, it is known as the crime of Cyber Terrorism. Generally, it includes the well-planned attack strategies on the Government and corporate computer system.
- **Cyberbullying** - When a teenager or adolescent harasses, defames, or intimidates someone with the use of the internet, phone, chat rooms, instant messaging or any other social network then the person is said to be committing the crime of Cyberbullying. When the same crime is done by adults it is known as Cyberstalking.
- **Hacking** - The most common cybercrime is Hacking. In this crime, the person gets access to other people's computers and passwords to use it for their own wrongful gain.
- **Defamation** - While every individual has his or her right to speech on internet platforms as well, but if their statements cross a line and harm the reputation of any individual or organization, then they can be charged with the Defamation Law.
- **Copyright** - With the massive surge in internet users, when the data/ information is distributed on all platforms, copyrighting your work aids you to restrict the use of your work. Any use of your copyrighted without your permission is a punishable offence.
- **Trade Secrets** - Internet organization spends a lot of their time and money in developing softwares, applications, and tools and rely on Cyber Laws to protect their data and trade secrets against theft; doing which is a punishable offence.
- **Freedom of Speech** - When it comes to the internet, there is a very thin line between freedom of speech and being a cyber-offender. As freedom of speech enables individuals to speak their mind, cyber law refrains obscenity and crassness over the web.
- **Harassment and Stalking** - Harassment and stalking are prohibited over internet platforms as well. Cyber laws protect the victims and prosecute the offender against this offence.

Top 5 Cybercrimes and Prevention Tips



1. Phishing Scams

The majority of successful cyberattacks – 91% according to a study by PhishMe – begin when curiosity, fear, or a sense of urgency entices someone to enter personal data. Phishing emails mimic messages from someone you know or a business that you trust. They are designed to trick people into giving up personal information or clicking on a malicious link that downloads

malware. Thousands of phishing attacks are launched every day.

What you can do: Stop trusting your emails. They are not always what they seem. Security awareness and Phishing training can empower your team to defend against phishing attacks by showing the telltale signs and teaching them how to recognize targeted phishing campaigns and malicious links and encouraging them to stay away from links and attachments and go directly to websites by typing the real URL into their browser.

2. Website Spoofing

The word spoof means to hoax, trick, or deceive. Website spoofing is when a website is designed to look like a real one and deceive you into believing it is a legitimate site. This is done to gain your confidence, get access to your systems, steal data, steal money, or spread malware.

Website spoofing works by replicating a legitimate website with a big company's style, branding, user interface, and even domain name in an attempt to trick users into entering their usernames and passwords. This is how the bad guys capture your data or drop malware onto your computer. Spoofed websites are generally used in conjunction with an email that links to the illegitimate website. Website spoofing resulted in $1.3 billion in losses last year according to the ***2019 Thales Access Management Index*** – cited in this article by Dr. Salvatore Stolfo.

What you can do: The easiest thing you can do is ignore and delete anything you're not anticipating. Legitimate companies will have multiple ways to contact you in the event they need to reach you. Save time and frustration by applying common sense logic and evaluating the "urgency" of the message. Also, pick up the phone or go directly to the trusted domain to inquire.

3. Ransomware

Ransomware is a modern day, technical twist on a crime that has been around for ages – extortion. At its core, ransomware works when criminals steal something of great value and demand payment in exchange for its return. For most businesses, this involves the encryption of

company data. When ransomware hits, businesses come to a standstill, and employees cannot do their jobs. Without restorable back-up data, the company is generally at the mercy of the attacker who will hold your data hostage in exchange for a decryption key you can buy with Bitcoin.Ransomware has matured into its own category of malware and should be a primary concern for all organizations.
McAfee reported that new ransomware attacks grew 118% between 2018 and 2019.

What you can do: Back your data up and then do it again... in a separate location. Frequency and redundancy are key to your success. If you only back up your system weekly, or if your backup is infected, you're in for a lot of trouble.

4. Malware

Norton defines malware as "malicious software" specifically designed to gain access to or damage a

computer. In the case of ransomware, it's designed to hold your data hostage, but that isn't the only kind. There can be multiple objectives for malware – power, influence, money, information – but the result is always the same – a time consuming, often expensive recovery effort.

Common types of malware include:

- Viruses that spread, damage functionality, and corrupt files
- Trojans disguised as legitimate software that quietly create backdoors to let other malware into your network
- Worms that can infect all of the devices connected to a network
- Ransomware that holds your data hostage
- Botnets – a network of infected devices that work together under the control of an attacker

What you can do: Be cautious about email attachments, avoid suspicious websites (look at the spellings carefully), install and continually update a high-quality antivirus program.

5. IOT Hacking

The Internet of Things is a brave new world that has opened insights into our daily routines and our business processes to the web. Whether we like it or not, all of these internet-connected objects are collecting and exchanging data. As you know, data is valuable and for that reason, hackers will look to exploit any devices that aggregate it.The more "things" we connect – the juicier the reward becomes for hackers. That's why it's important to remember that personal passwords and business passwords all belong to humans… with memories that we know are going to let us down from time to time.

What you can do: Use a password generator to secure all devices with unique passwords. Here's a list of the top 10 password managers you can use to help you keep your devices more secure.

Remember, while you're working within a business, each person has to take personal responsibility for ensuring your cybersecurity. You have to prioritize your risks and think through the scenarios that are likely to affect you, based on what you know about your unique infrastructure and team. Don't wait until it's too late to take a proactive approach. Keep focused on what's coming and work to bring your team up to speed to create the strongest defense against cyberattacks.

CATEGORIES OF CYBERCRIME

- **Individual**- Cybercrimes against individuals involve crimes like online harassment, distribution and trafficking of child pornography, manipulation of personal information, use of obscene data, and identity theft for personal benefit.

- **Property**- Usage, and transmission of harmful programs, theft of information and data from financial institutions, trespassing cyberspace, computer vandalism, and unauthorized possession of information digitally are some of the crimes under the property.
- **Government**- The crimes that come under this are cyber terrorism, manipulation, threats, and misuse of power against the Government and citizens. Groups or Individuals terrorizing Government websites is when this form of cyber terrorism occurs.

CYBER LAWS

Cyber law is also known as Cyber Law or Internet Law. Cyber law India is the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, hardware and information systems (IS).

Internet law or Cyber law India is a term that encapsulates the legal issues related to use of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation. Some leading topics include internet access and usage, privacy, freedom of expression, and jurisdiction

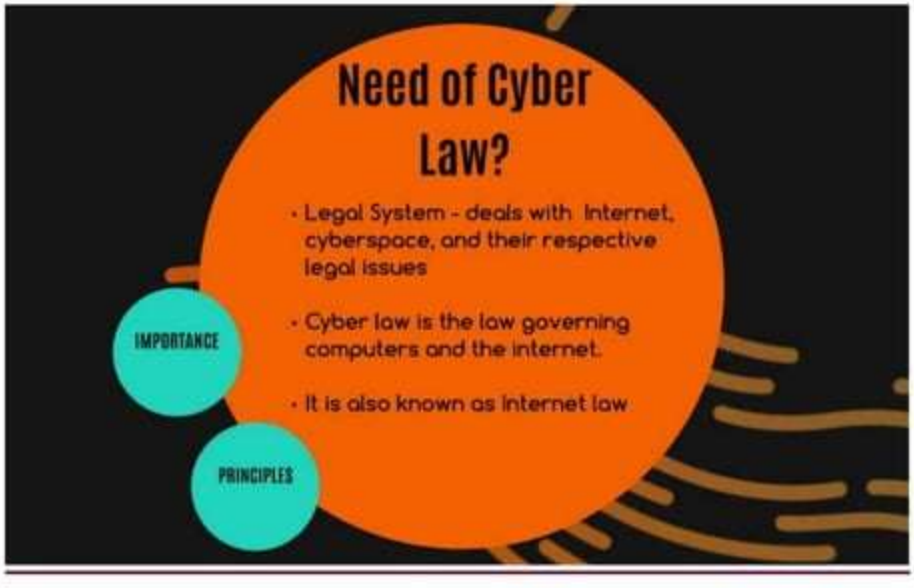
Thus Cyber law India can consider as a part of the overall legal system that deals with the Internet, E-commerce, digital contracts, electronic evidence, cyberspace, and their respective legal issues. Cyber law India covers a fairly broad area, encompassing several subtopics including freedom of expression, data protection, data security, digital transactions, electronic communication, access to and usage of the Internet, and online privacy.

THE IMPORTANCE OF CYBER LAW

Just like any other law, Cyber law consists of rules that dictate how people and companies should use the internet and computers. While other rules protect people from getting trapped in Cybercrime run by malicious people on the internet. Although it is close to impossible to curb 100% of all cybercrimes, laws implemented all around the world assist Now the question arises, what are Cyber law and its importance? The importance of Cyber law can be understood by the following points:

- It dictates all actions and reactions in Cyberspace.
- All online transactions are ensured to be safe and protected
- All online activities are under watch by the Cyber law officials.
- Security for all data and property of individuals, organizations, and Government
- Helps curb illegal cyber activities with due diligence
- All actions and reactions implemented on any cyberspace has some legal angle associated with it
- Keeps track of all electronic records
- Helps to establish electronic governance

NEED OF CYBER LAW



As of early 2021, the number of people that use the internet is over 4.66 Billion. With that number increasing by 7% annually. This also means every day can account for almost 8,75,000 new users. Given this swift increase in the use of Cyberspace, implementation and the usage of strict cyber rules helps establish a safe and secure environment for the users. Living in a rapidly progressing world, the one thing to keep pace with it is the Internet.

THE VARIOUS COMPONENTS OF CYBER LAW

Safeguarding data and privacy– Both private and professional information and data must be secured thoroughly. Personal and financial information always attracts cybercriminals. Misuse of this information by any other person is illegal and that is where these laws come into play. The basic steps to safeguard your data and privacy is elaborated below

Two-factor authentication for financial platforms and any other forums that provide this function.

- Initiate Virus protection software.
- Use only verified payment methods on reputed websites.
- Avoid giving out personal information

Cybercrimes- These crimes are any illegal activities that occur on a networked technological device. These crimes include online and network attacks, extortion, harassment, money laundering, hacking, and many more.

Intellectual property- Intellectual property is basically an individual or group's work, designs, symbols, inventions, or anything owned by them which are intangible and are usually patented or copyrighted. Now cyber theft would mean the stealing or illegal use of the same intangible items.

Electronic and digital signatures- Nowadays most individuals and companies use electronic signatures to verify electronic records. This has become reliable and regular. The wrong usage by another of this signature is illegal and hence a cybercrime.

TYPES OF CYBER LAW

Some major types of Cyber Law are:

- **Copyright:** These days' copyright violations come under Cyber law. It protects the rights of companies and individuals to get profit from their creative work. In earlier days, online copyright violation was easier. But due to the introduction of Cyber law, it has become difficult to violate copyright. Which is very good!
- **Defamation:** Generally, people use the internet to speak out their minds. But in the case of fake public statements on the internet that

are bound to hamper someone's business and reputation, that is when defamation law comes into the picture. Defamation Laws are a kind of civil law.

- **Fraud:** What is Cybercrime law? The major motive of this law is to protect people from online fraud. Consumers these days depend on Cyber Law to prevent online fraud. IT law prevents credit card theft, identity theft, and other money-related crimes that are bound to happen online. People who commit online fraud, face state criminal charges. They may also witness a civil action by the victim.
- **Harassment and Stalking:** Some statements made by people can violate criminal law that refuses stalking and harassment online. When somebody posts threatening statements repeatedly about somebody else, this violates both criminal and civil laws. Cyber lawyers fight and defend people when online stalking occurs.
- **Freedom of Speech:** The internet is used as a medium of free speech. But there are laws to avoid free speech that may cause immorality online. Cyber lawyers should advise their clients about the amount of free speech allowed online. Sometimes the Cyber lawyers fight cases for their clients where they debate whether their client's actions are within the permissible limit of free speech.
- **Trade Secrets:** Businesses depend on Cyber laws to preserve their trade secrets. For example, some organizations might steal online algorithms or features designed by another firm. In this case, Cyber laws empower the victim organization to take legal action to protect its secrets.
- **Contracts and Employment Laws:** You might have agreed upon many terms and conditions while opening a website or downloading some software. This is where the Cyber law is used. These Terms & Conditions are designed for online privacy concerns.

Cyber law came with the major objective to maintain law and order in all kinds of online activities and reduce Cybercrime. There are other objectives of Cyber Law as well. These will help you understand Cyber law better. These are:

- Unlike paper-based communication, the legal recognition of all the transactions via electronic media whether data or e-commerce is granted by the Cyber law.
  - Digital Signatures became legal only due to the introduction to Cyber law.
- One of the biggest advantages of Cyber Law is that it facilitates the e-filing of documents with Government departments and agencies.
- It also grants legal sanctions and also allows electronic fund transfer between financial institutions and banks.
- It also legally authorizes the bankers to keep the books of accounts in electronic form.

IMPACT OF COVID ON CYBER-SAFETY

Although strict laws have been implemented, due to the pandemic there has been a drastic increase in the use of online financial transaction methods which has, in turn, led to an increase in frauds. The education and health sector has also undergone severe attacks after the pandemic hit. There has also been a hike of 500% in the number of security breaches that have affected many in India after the lockdown was announced.

ADD-ONS TO THE CYBER LAW IN INDIA AS OF 2021

With social media being the new-found forum for everyone to communicate and express their views, the Government of India has established new rules to regulate social media and OTT (over-the-top) platforms. It was duly established to curb the usage and propagation of hate speech. Another crucial reason is to address grievances people have faced. They will also track inappropriate messages and tweets to the first originator. This will be done by the Government or a court order

directed to that particular platform. The Government also made it ascertain that they will not encourage anything that could be a possible threat to National Security.

The need for Social Media and OTT directives

- Defamation and hate speech- Due to the sudden rise of visibility on social media, it is imperative to curb hate speech and defamation as it can have severe implications on the public.
- Misuse of content and misinformation- Another major issue is the misuse of personal content and even obscene content on the same platforms.
- Online Protection- Need for protecting women and men from sexual offenses that occur on these platforms.

There were no previously effective rules that ensured the content-driven on OTT Platforms were watched by an appropriately aged audience or not. However, now with the new rules & strict parent locks content will be delivered to the right audience

DRAWBACKS OF THIS NEW AMENDMENT

- Privacy Concerns- Any information can be misused and the usage of propaganda of any sorts can affect digital publishers
- Contradicting the Right to Freedom of Speech and Expression- According to Article 19(a), this right allows citizens to express any opinion on any channel of communication, be it speech or writing. Curbing and regulating social media is basically stripping citizens of their Right to freedom of speech and expression.
- Issues with tracking- For the Government to track hate speech and first originators of tweets, personal data like WhatsApp messages is required. But the question arises of how they will be able to derive such information when WhatsApp is encrypted.

Although all of the above mentioned has been announced by the Government the formal version of the guidelines will be published in the coming months for a detailed understanding.

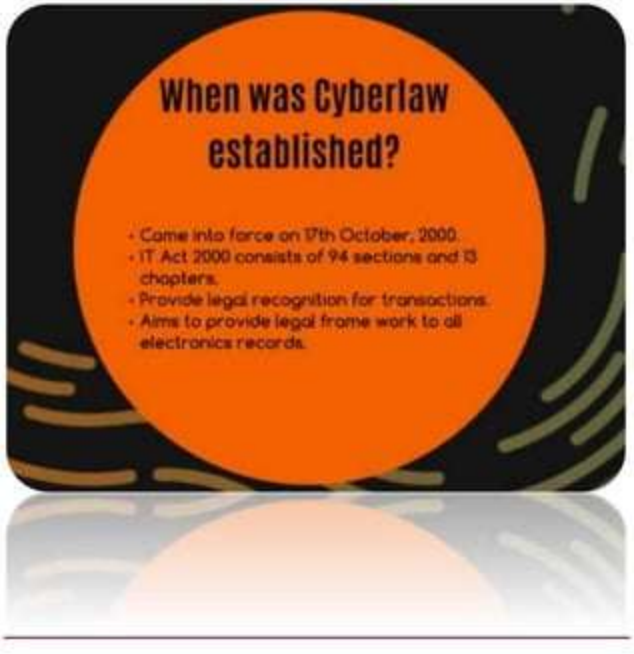
APART FROM THE IT ACT OF 2000, THERE ARE OTHER LAWS THAT ENTAIL CYBERSECURITY WHICH ARE-

- Companies Rules 2014 under the Companies Act 2013, makes it mandatory for all companies to ensure that all digital records and security systems are tight and sealed to avoid tampering and illegal access
- The Indian Penal Code Act 1860 punishes any crime committed in cyberspace (such as cheating, harassment, hacking, breach of privacy, etc)
- Sector-specific regulations are also established in The department of telecommunication, The Reserve Bank of India, and the Insurance Regulatory. Strict cybersecurity rules have been implemented

INCENTIVES PROVIDED BY THE GOVERNMENT TO INCREASE CYBERSECURITY AMONG COMPANIES

The Government has provided some beneficial measures for both public and private sector organizations to increase their standards of cybersecurity. One is the Public Procurement Order 2018 for Cyber Security Products where cybersecurity was named a strategic sector. It further mentioned that government agencies will prefer cybersecurity products that will be procured from domestically manufactured entities

INTRODUCED



These two pieces of legislation form the bedrock of cyberlaw infrastructure in India.

The Information Technology (IT) Act, 2000 was passed by the Indian Parliament in May 2000 and came into force in October of the same year. Its prime purpose is to provide the legal infrastructure for e-commerce in India. It was the first legal instrument to provide legal sanctity to electronic records and contracts expressed through electronic means of communication.

The act was later amended in December 2008 through the IT (Amendment) Act, 2008. Some of their salient points are:

- **Digital Signatures:** Electronic records may be authenticated by a subscriber by affixing digital signatures; further, the signature may be verified using the public key provided by the subscriber

- **Certifying Authorities:** domestic and foreign certifying authorities (which provide digital signature certificates) are recognized by the law; a "Controller of Certifying Authorities" shall supervise them

- **Electronic governance:** Documents required as per law by any arm of the government may be supplied in electronic form, and such documents are to be treated the same as handwritten, typewritten or printed documents

- **Offences and Penalties:** An Adjudicating Officer shall judge whether a person has committed an offence in contravention of any provision of the IT Act, 2000; the maximum penalty for any damage to computers or computer systems is a fine up to `1 crore

- **Appellate Tribunals:** A Cyber Regulations Appellate Tribunal shall be formed which shall hear appeals against orders passed by the Adjudicating Officers

- **Investigation:** Offences shall only be investigated by a police officer of the rank of the Deputy Superintendent of Police or above (amended to the rank "Inspector" or above by the IT (Amendment) Act, 2008)

- **Amendments to other laws:** Other acts such as the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Bankers' Books

Evidence Act, 1891, the Reserve Bank of India Act, 1934 were to be amended to align them with the IT Act

- **Network Service Providers:** Intermediaries in the data transmission process, such as Internet Service Providers, are not liable in certain cases, so long as the intermediary expeditiously acts to prevent the cybercrime on getting such instruction from the Government or its agency.

CYBER LAWS THAT EVERYONE USING THE INTERNET MUST BE AWARE OF

Internet is just like life. It is interesting and we spend a lot of time doing amusing things here, but it comes with its fair share of trouble. With the technology boom and easy Internet access across the country, cyber crime, too, has become a pretty common occurrence. From hacking into computers to making fraudulent transactions online, there are many ways in which we can become a victim of illegal cyber activities.

To regulate such activities that violate the rights of an Internet user, the Indian government has the Information Technology Act, 2000, in place. Here are some of its sections that empower Internet users and attempt to safeguard the cyberspace.

SECTION 65- TAMPERING WITH COMPUTER SOURCE

A person who intentionally conceals, destroys or alters any computer source code (such as programmes, computer

commands, design and layout), when it is required to be maintained by law commits an offence and can be punished with 3 years' imprisonment or a fine of 2 Lakhs INR or both

SECTION 66- USING PASSWORD OF ANOTHER PERSON

If a person fraudulently uses the password, digital signature or other unique identification of another person, he/she can face imprisonment up to 3 years or/and a fine of 1 Lakh INR.

SECTION 66D- CHEATING USING COMPUTER RESOURCE

If a person cheats someone using a computer resource or a communication device, he/she could face imprisonment up to 3 years or/and fine up to 1 Lakh INR

SECTION 66E- PUBLISHING PRIVATE IMAGES OF OTHER

If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge, the person is entitled to imprisonment up to 3 years of fine up to 2 Lakhs INR or both

SECTION 66F-ACTS OF CYBER TERRORISM

A person can face life imprisonment if he/she denies an authorized person the access to the computer resource or

attempts to penetrate/access a computer resource without authorization, with an aim to threaten the unity, integrity, security or sovereignty of the nation. This is a non-bailable offence.

SECTION 67- PUBHLISHING CHILD PORN OR PREDATING CHILDREN ONLINE

If a person captures, publishes or transmits images of a child in a sexually explicit act or induces anyone under the age of 18 into a sexual act, then the person can face imprisonment up to 7 years or fine up to 10 lakhs INR or both

SECTION 69- GOVT'S POWER TO BLOCK WEBSITES

If the government feel it necessary in the interest of sovereignty and integrity of India, it can intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. The power is subject to compliance of procedure. Under section 69A, the central government can also block any information from public access.

SECTION 43A- DATA PROTECTION OF CORPORATE LEVELS

If a body corporate is negligent in implementing reasonable security practices which causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages to the affection person.

INDIAN PENAL CODE (IPC) 1980

Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000. The primary relevant section of the IPC covers cyber frauds:

- **Forgery (Section 464)**
- **Forgery pre-planned for cheating (Section 468)**
- **False documentation (Section 465)**
- **Presenting a forged document as genuine (Section 471)**
- **Reputation damage (Section 469)**

INDIAN PENAL CODE 1860

COMPANIES ACT OF 2013

The corporate stakeholders refer to the Companies Act of 2013 as the legal obligation necessary for the refinement of daily operations. The directives of this Act cements all the required techno-legal compliances, putting the less compliant companies in a legal fix.

The Companies Act 2013 vested powers in the hands of the SFIO (Serious Frauds Investigation Office) to prosecute Indian companies and their directors. Also, post the notification of the Companies Inspection, Investment, and Inquiry Rules, 2014, SFIOs has become even more proactive and stern in this regard.

The legislature ensured that all the regulatory compliances are well-covered, including cyber forensics, e-discovery, and cybersecurity diligence. The Companies (Management and Administration) Rules, 2014 prescribes strict guidelines confirming the cybersecurity obligations and responsibilities upon the company directors and leaders.

NIST COMPLIANCE

The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), offers a harmonized approach to cybersecurity as the most reliable global certifying body. NIST Cybersecurity Framework encompasses all required guidelines, standards, and best practices to manage the cyber-related risks responsibly. This framework is prioritized on flexibility and cost-effectiveness. It promotes the resilience and protection of critical infrastructure by:

- **Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs**
- **Determining the most important activities and critical operations - to focus on securing them**
- **Demonstrates the trust-worthiness of organizations who secure critical assets**
- **Helps to prioritize investments to maximize the cybersecurity ROI**
- **Addresses regulatory and contractual obligations**
- **Supports the wider information security program**

By combining the NIST CSF framework with ISO/IEC 27001 - cybersecurity risk management becomes simplified. It also makes communication easier throughout the organization and across the supply chains via a common cybersecurity directive laid by NIST.

Prominent cybercrime cases:

1. First conviction for a cybercrime in India

A call center employee at Noida had gained access to to an American citizen's credit card information and used the same to purchase a color television and a cordless phone through a Sony Entertainment website catering to NRIs. A month after the items were delivered to the individual, Sony Entertainment was informed by the credit card agency that the card owner had denied making the purchase. Luckily, digital photographs taken at the time of delivery were evidence enough for the CBI to convict the individual under several sections of the Indian Penal Code.

2. First conviction under the IT Act, 2000

Obscene and defamatory messages regarding a divorced woman were posted on a Yahoo message group, which resulted in phone calls to the woman in the belief that she was soliciting. Investigating based on a complaint made by the victim in February 2004, the police traced the source of the message to a Mumbai resident who was a family friend of the victim. He had resorted to harassing the victim as she had rejected his marriage offer. The accused's lawyers argued that the offending messages might have been sent by either the victim's ex-husband or by the victim herself in order to implicate the accused, and that the documentary evidence was not sustainable under the Indian Evidence Act. However, the court found the accused guilty based on the statements by the Cyber Cafe owner where the messages originated as well as expert witness provided by Naavi. The accused was sentenced to rigorous imprisonment for 2 years and find `5000.

3. Hackers deface the official website of the Maharashtra Government

The website http://www.maharashtra government.in, which contains details about government departments, circulars, reports, and several other topics, was hacked on 20 September 2007. Sources believed the hackers to be from Washington, USA, although, the hackers identified themselves as "Hackers Cool Al-Jazeera" and claimed they were based in Saudi Arabia, which authorities believe might be a red herring to throw investigators off their trail. Deputy Chief Minister and Home Minister R.R. Patil stated that, if needed, the government would seek help of private IT experts to find the hackers.

4. Online credit card scam solved; three held guilty

A bank employee who had access to credit card details of the banks customers used them along with two other individuals to book tickets online and sell them to third parties. According to the information provided by the police, the scam was detected when one of the customers received an SMS alert for purchasing an airline ticket even though he had the card on him and had not used it. The alert customer immediately informed the bank who then involved the police. Eight days investigation by Cyber Cell head DCP Sunil Pulhari, PI Mohan Mohadikar, and A.P.I Kate resulted in the arrests of the three involved.

5. Murder solved with aid from MySpace

The murder of a high school football player was solved when police found the prime suspect in a picture posted on a street gang's MySpace page.

FINAL THOUGHTS

As human dependence on technology intensifies, cyber laws in India and across the globe need constant up-gradation and refinements. The pandemic has also pushed much of the workforce into a remote working module increasing the need for app security.

Lawmakers have to go the extra mile to stay ahead of the impostors, in order to block them at their advent. Cybercrimes can be controlled but it needs collaborative efforts of the lawmakers, the Internet or Network providers, the intercessors like banks and shopping sites, and, most importantly, the users. Only the prudent efforts of these stakeholders, ensuring their confinement to the law of the cyberland - can bring about online safety and resilience.

THANK YOU