Parul® University

Fundamentals of Information Security

Prof. Rakshith

CHAPTER-2

Introduction

Why is this unit required?

- Addressing ethical concerns is crucial in cybersecurity to ensure responsible and secure technology use.
- Understanding ethics in cybersecurity helps professionals make morally sound decisions.
- Ethical guidelines can prevent misuse of technology, such as hacking for malicious purposes.
- Cyberbullying awareness is essential to protect individuals from online harassment and its emotional consequences.
- Identifying warning signs of cyberbullying victims enables timely intervention and support.
- Knowledge of applicable laws in cybersecurity is vital to ensure legal compliance and accountability.
- Ethical considerations and laws help create a safer and more responsible digital environment.
- A focus on ethics enhances public trust in technology and the security of digital systems.

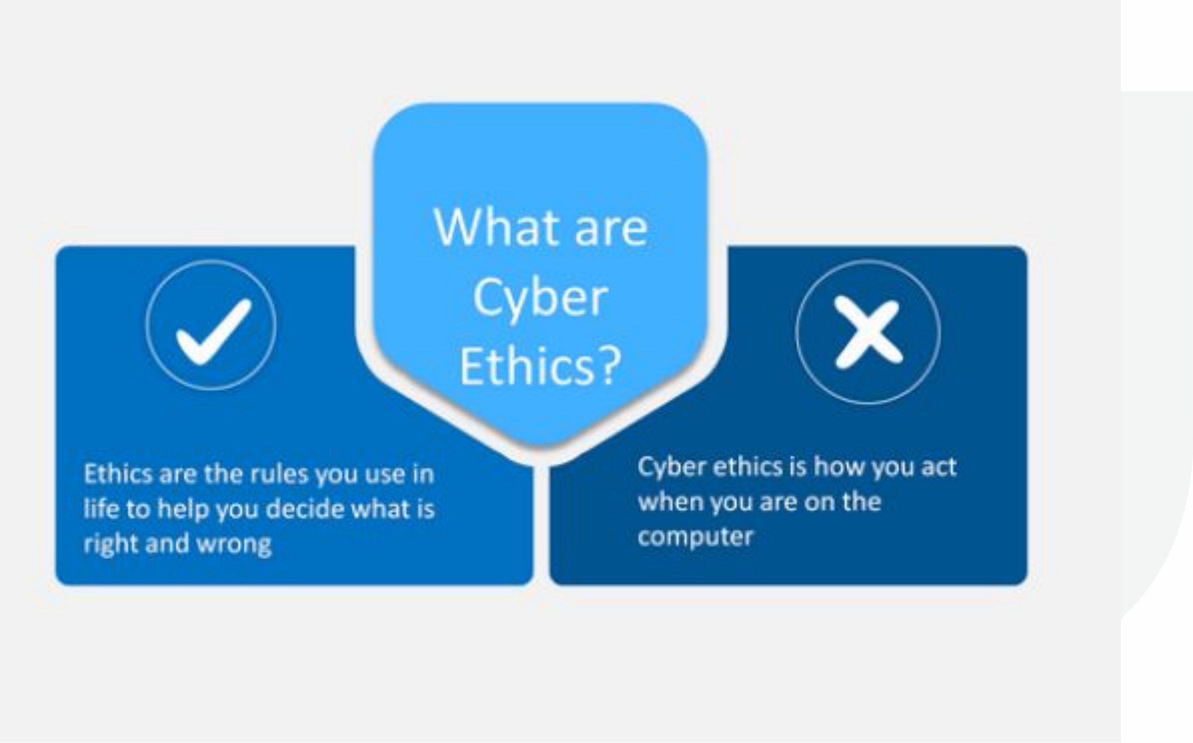
What is Ethics?

- Ethics is a branch of philosophy that deals with the study of what is morally right and wrong. It involves examining and understanding principles, values, and rules that govern human behavior and decision-making in various contexts.

What is Cyber ethics?

- Internet ethics or computer ethics, is a branch of applied ethics that focuses on ethical issues and dilemmas related to the use of technology, particularly in the context of the internet and digital environments.
- It addresses the moral and ethical considerations that arise from the use of computers, the internet, and digital technology

Difference Ethics vs Cyber Ethics?



What are Cyber Ethics?

✓ Ethics are the rules you use in life to help you decide what is right and wrong

✗ Cyber ethics is how you act when you are on the computer

Primary ethical concerns within the field of cyber ethics include:?

- **Privacy:** Concerns related to the collection, storage, and use of personal data in the digital age. This includes issues such as data breaches, online surveillance, and the responsible handling of user information.
- **Cybersecurity:** Ethical considerations regarding the protection of digital systems and data. This includes the responsible management of security vulnerabilities and the prevention of cyberattacks.
- **Intellectual Property:** Questions about intellectual property rights in the digital world, including issues of copyright infringement, software piracy, and plagiarism.
- **Online Behavior:** Ethical issues surrounding behavior on the internet, such as cyberbullying, trolling, online harassment, hate speech, and the spread of false information.

Primary ethical concerns within the field of cyber ethics include:?

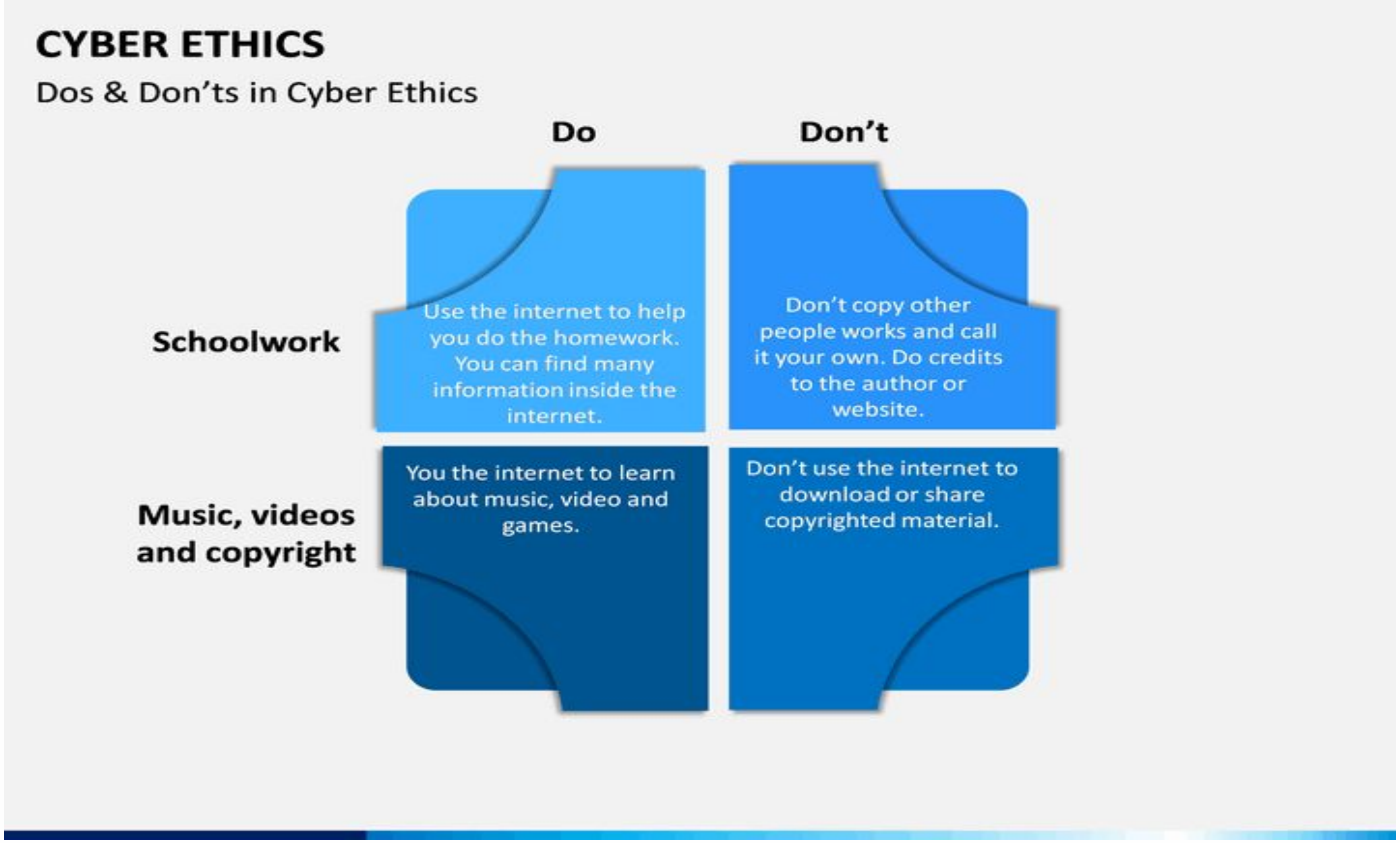
- **Cybercrime:** Ethical considerations related to illegal online activities, such as hacking, identity theft, fraud, and the distribution of malicious software.

- **Online Communities:** Ethical behavior within online communities, social networks, and virtual spaces. This includes issues like online activism, digital advocacy, and the ethical use of social media.

- **Artificial Intelligence (AI):** Ethical implications of AI and machine learning, including issues related to algorithmic bias, automated decision-making, and the responsible development and use of AI systems.

Primary ethical concerns within the field of cyber ethics include:?

Do’s and Don’t’s

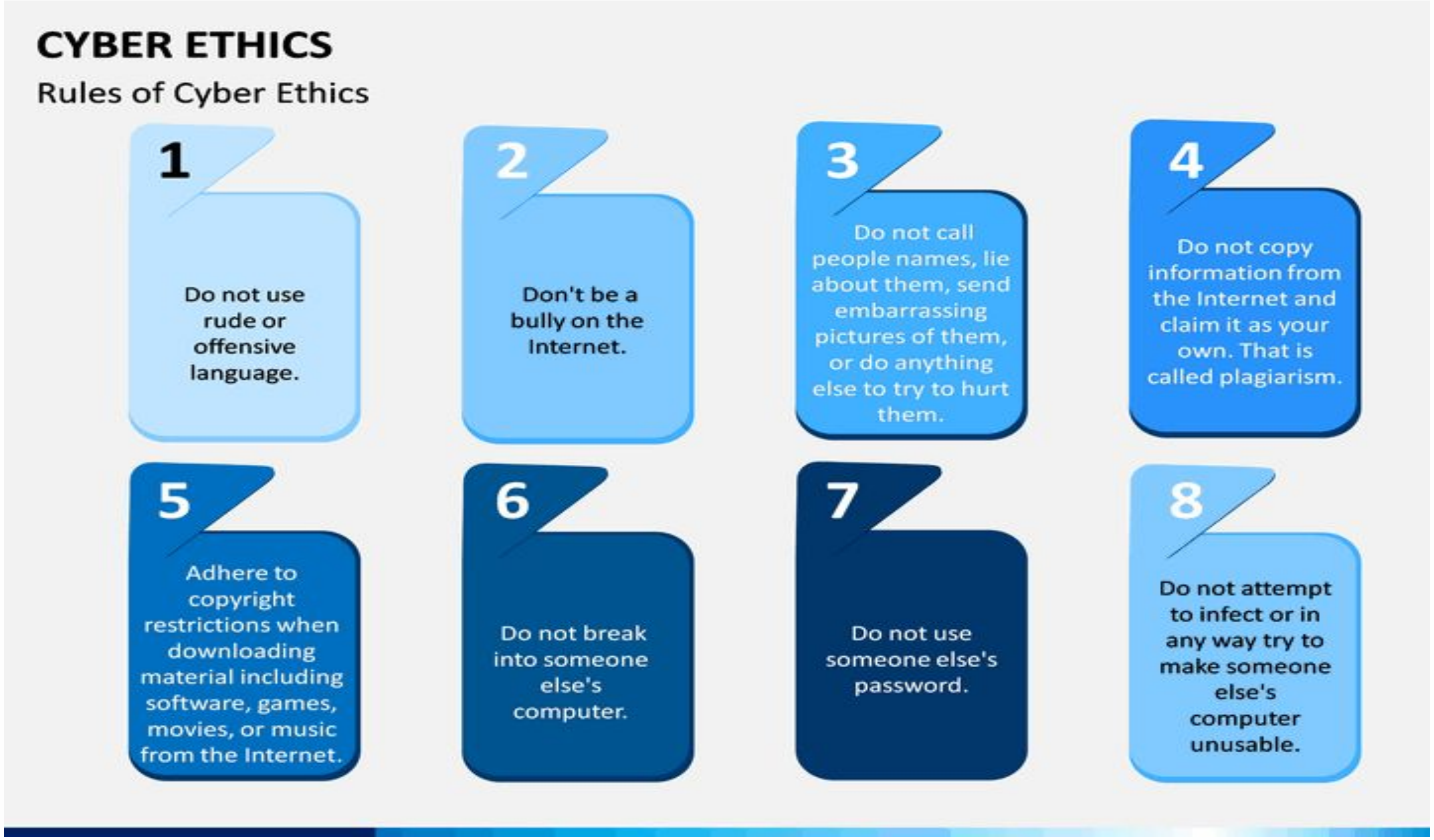


CYBER ETHICS

Dos & Don’ts 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	You the internet to learn about music, video and games.	Don’t use the internet to download or share copyrighted material.

RULES of Cyber Ethics?



CYBER ETHICS

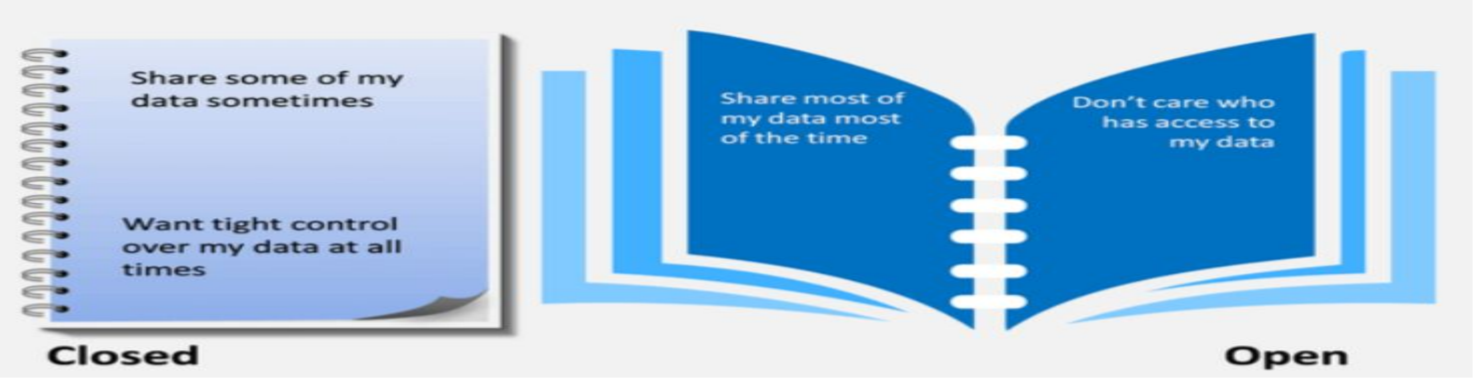
Rules of Cyber Ethics

1. Do not use rude or offensive language.
2. Don't be a bully on the Internet.
3. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
4. Do not copy information from the Internet and claim it as your own. That is called plagiarism.
5. Adhere to copyright restrictions when downloading material including software, games, movies, or music from the Internet.
6. Do not break into someone else's computer.
7. Do not use someone else's password.
8. Do not attempt to infect or in any way try to make someone else's computer unusable.

Some examples to undertsand ?

Privacy: "The Personal Data Leak"

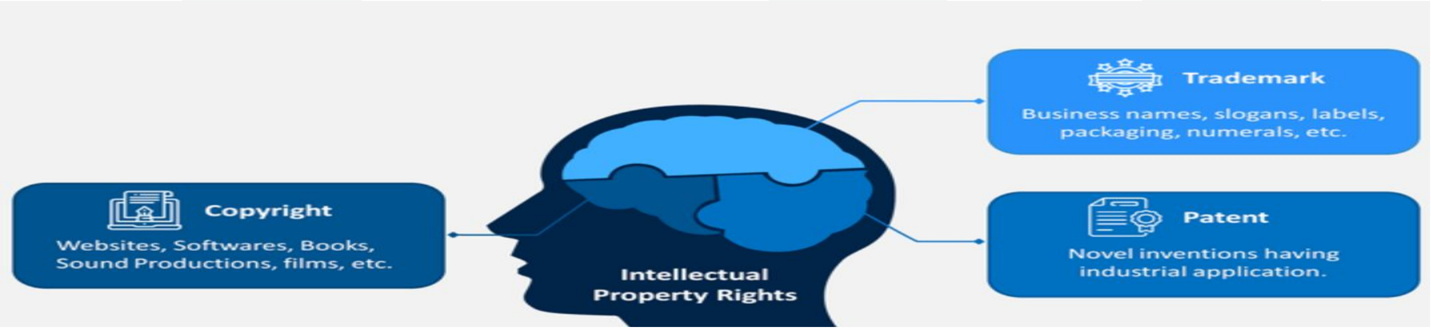
Imagine you're developing a new app for your B.Tech project, and it requires users to sign up with their personal information. You need to ensure that the users' data, like their names and email addresses, is kept safe. If someone were to hack into your app's database and steal all that personal data, it would be a breach of privacy. Protecting this information is vital to respecting the privacy of your users.


Share some of my data sometimes
Want tight control over my data at all times
Share most of my data most of the time
Don't care who has access to my data
Closed
Open

Some examples to undertsand ?

Intellectual Property: "The Code Copycat"

Suppose you've spent countless hours writing a complex piece of code as part of your B.Tech project. You've documented it well and published it online to share with the programming community. However, another student finds your code, copies it without giving you credit, and claims it as their own work. This is an example of intellectual property infringement, where your original creation is not respected or attributed to you.



Copyright

Websites, Softwares, Books, Sound Productions, films, etc.

Intellectual Property Rights

Trademark

Business names, slogans, labels, packaging, numerals, etc.

Patent

Novel inventions having industrial application.

What is LAW?

- **Law** is a system of rules and regulations that are created and enforced by a recognized authority, typically a government, to regulate behavior within a society.
- Or
- A comprehensive system of rules and regulations, serves as the foundation for social order, offering guidelines for individual and collective conduct while enforcing justice through governing authorities.

What is CYBER LAW?

- Internet law or digital law, is a specialized field of law that deals with legal issues related to the use of the internet, digital technology, and information technology.

Difference between ethics and cyber law's?

Aspect	Cyber Ethics	Cyber Law
Definition	Cyber ethics refers to the moral principles and guidelines that govern the behavior of individuals and organizations in the digital realm.	Cyber law encompasses the legal regulations and statutes that govern and enforce activities in cyberspace.
Nature	Voluntary and self-imposed principles that guide ethical behavior online.	Mandated and enforced by government authorities and legal systems.
Compliance	Adherence is a matter of personal and professional integrity, often not legally enforced.	Non-compliance may result in legal actions, penalties, and consequences.

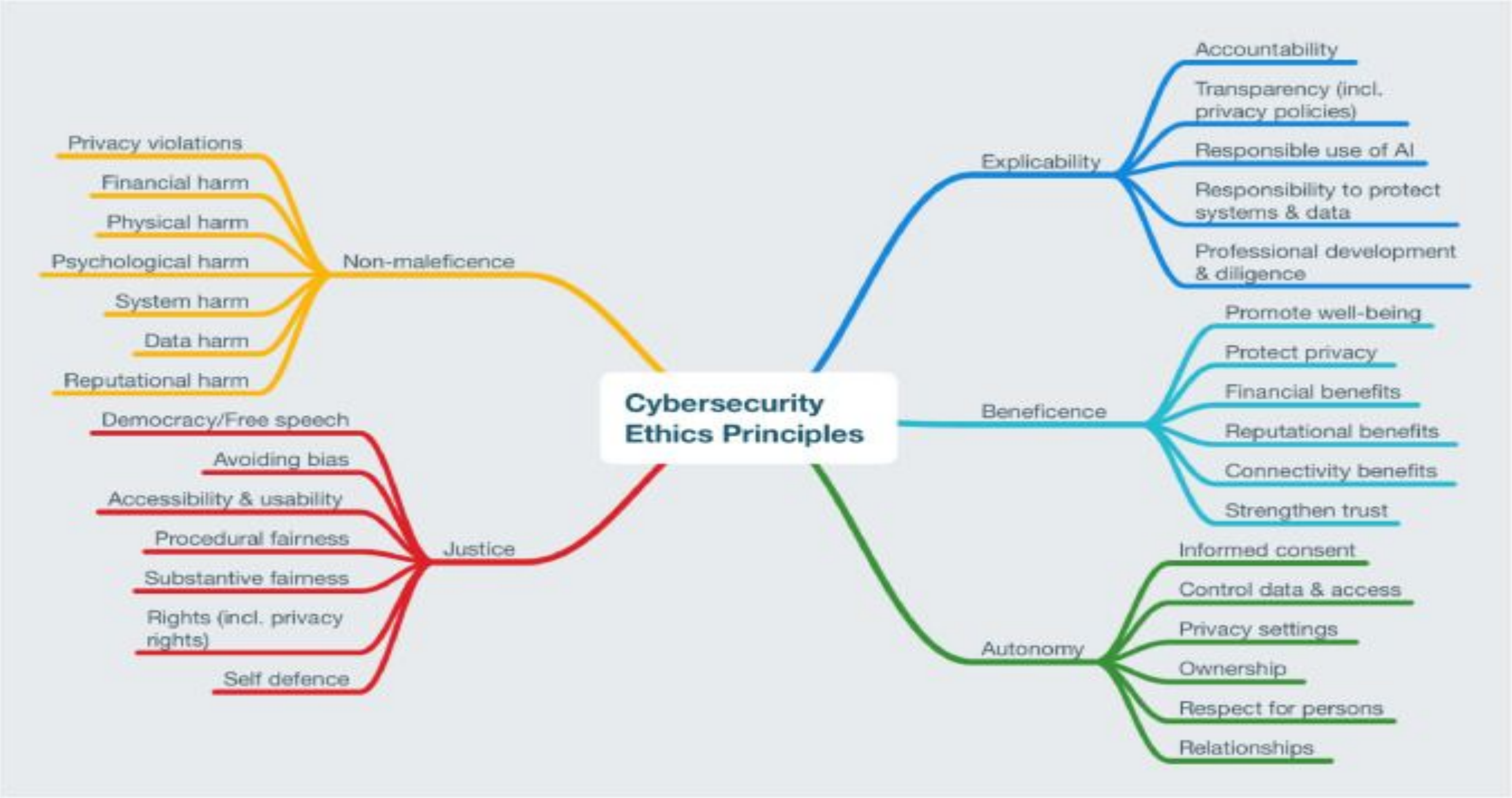
Difference between ethics and cyber law’s?

Scope	Focuses on individual and organizational behavior, emphasizing values and norms.	Covers a broader range of issues, including data privacy, intellectual property, cybercrime, and more.
Purpose	Promotes responsible and ethical behavior online, considering the well-being of individuals and society.	Establishes rules and regulations to maintain order, protect rights, and address legal issues in cyberspace.
Enforcement	Enforced by social pressure, peer influence, and reputation.	Enforced by government agencies, courts, and legal authorities.

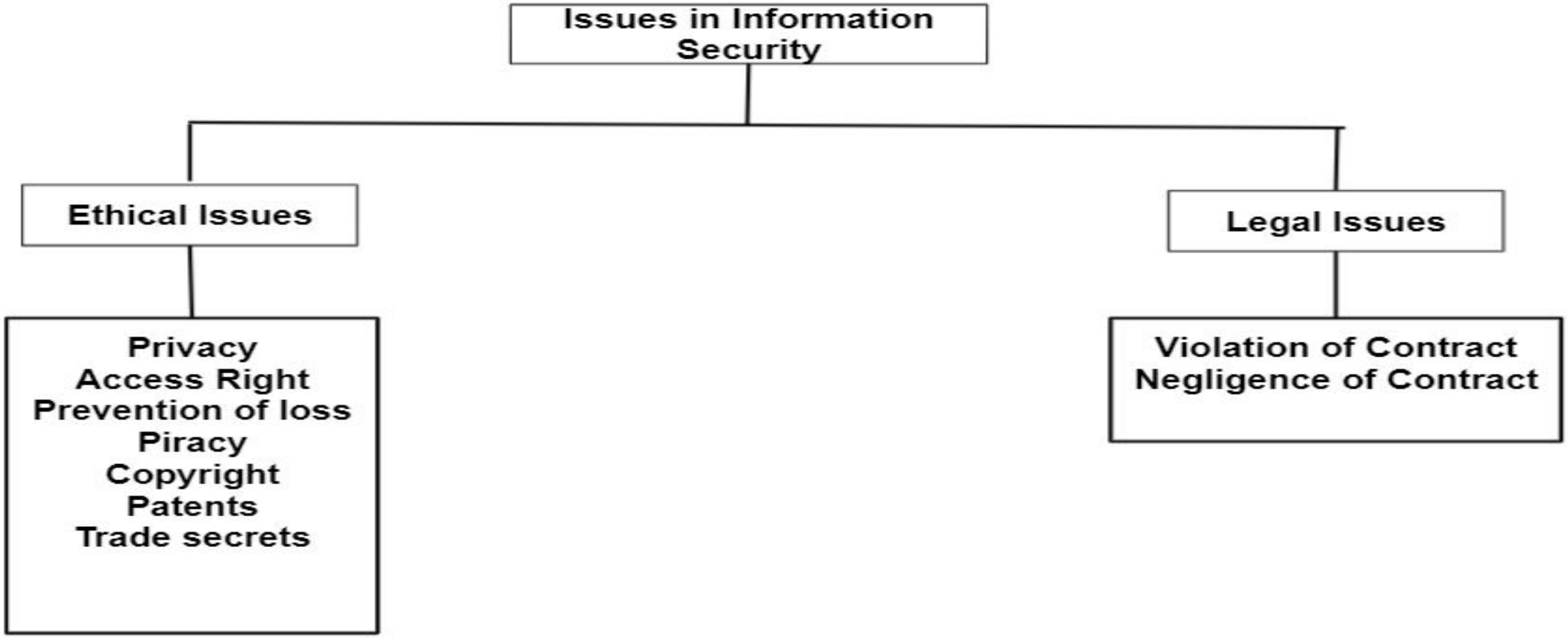
Difference between ethics and cyber law’s?

Examples	Respect for online privacy, not engaging in cyberbullying, practicing good netiquette.	Laws against hacking, copyright infringement, online fraud, and other cybercrimes.
Flexibility	More flexible and adaptable to evolving technology and social norms.	Can be rigid and slow to adapt to changing technology, requiring legislative updates.
Global Consistency	Cultural and regional variations can influence ethical standards.	Laws may vary from one jurisdiction to another, causing legal discrepancies.
Punishments/Consequences	Consequences may include damage to reputation, exclusion from online communities, or social ostracism.	Legal consequences may include fines, imprisonment, or other legal penalties.

Ethical Issues in Cyber Security



Ethical Issues in Cyber Security



Issues in Information Security

Ethical Issues

Privacy
Access Right
Prevention of loss
Piracy
Copyright
Patents
Trade secrets

Legal Issues

Violation of Contract
Negligence of Contract

Define Cyberbullying

- **Cyberbullying** is a form of **harassment**, **intimidation**, or **aggressive behavior** that takes place in digital or online environments. It involves using electronic communication tools, such as social media, instant messaging, email, or other digital platforms, to target and harm individuals, typically with the intention of causing emotional **distress, humiliation, or harm**.

Cyberbullying can manifest in various ways

1.**Harassment:** Repeatedly sending hurtful or threatening messages to an individual.

2.**Flaming:** Engaging in heated, aggressive, and disrespectful online arguments or exchanges.

3.**Exclusion:** Intentionally excluding someone from online groups or conversations.

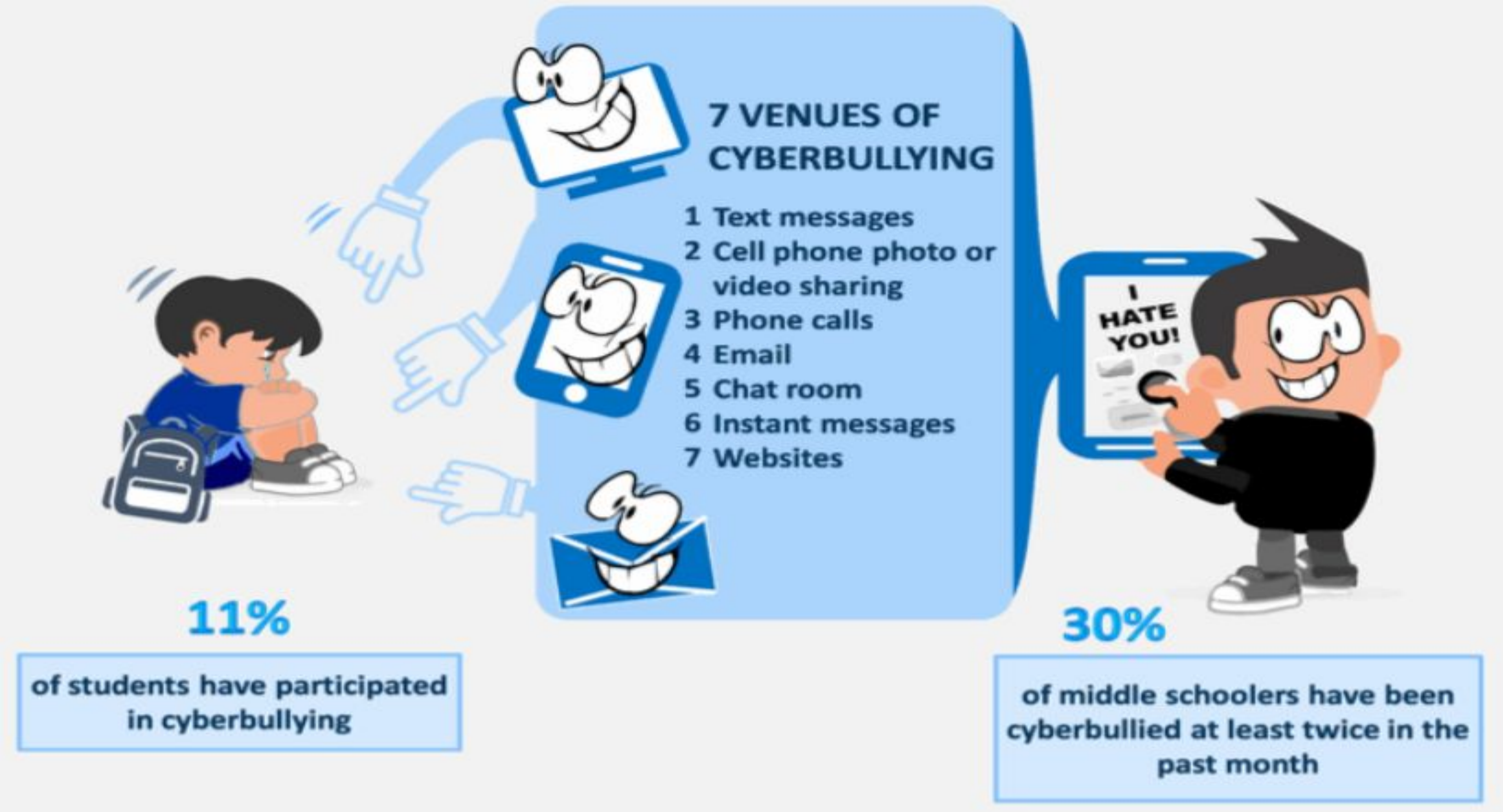
4.**Outing:** Sharing personal, private, or embarrassing information about someone without their consent.

5.**Impersonation:** Pretending to be someone else online to deceive or harm the target.

6.**Cyberstalking:** Relentlessly tracking or monitoring someone's online activities and personal life.

7.**Trolling:** Posting inflammatory or offensive comments online to provoke reactions and upset others.

Venues of cyberbullied



7 VENUES OF CYBERBULLYING

1 Text messages
2 Cell phone photo or video sharing
3 Phone calls
4 Email
5 Chat room
6 Instant messages
7 Websites

11%

of students have participated in cyberbullying

30%

of middle schoolers have been cyberbullied at least twice in the past month

Responding to cyberbullying

- https://cyberbullying.org/wp-content/uploads/2013/10/adult-cyberbullying-response.jpg

Punishments of Cyber Bullying

Section 66 A of the Information Technology Act, 2000:-

This section deals with the punishment for sending messages or emails which are harmful or abusive in nature through the internet or any other platform. These messages are sent to cause annoyance, injury, and inconvenience to the victim. It is also punishable under the provision when someone shares information that he believes to be false.

Sec 66 D of the Information Technology Act, 2000:-

An individual who cheats by personation using any social media or communication device is punished under this provision. It means a person is typically punished for fraudulently pretending to be some other person.

Examples of some cyber bullying

Fake Facebook Profiles

Creation of a Facebook profile in someone else's name is relatively easy and such a profile makes it possible to show the victim in a false light. There have been instances where vulgar or obscene photos of a victim have been linked to such fake Facebook profile, causing the victim extreme mental anguish.

When the creation of a fake Facebook profile is accompanied by the uploading of vulgar or obscene photos of the victim on to such profile, Section 354A (*Sexual harassment and punishment for sexual harassment*), Section 354D (*Stalking*), Section 499 read with Section 500 (*Defamation and Punishment for defamation*), Section 507 (*Criminal intimidation by an anonymous communication*) and Section 509 (*Word, gesture or act intended to insult the modesty of a woman*) of IPC may apply.

Examples of some cyber bullying

Bullying Inter-se School Mates

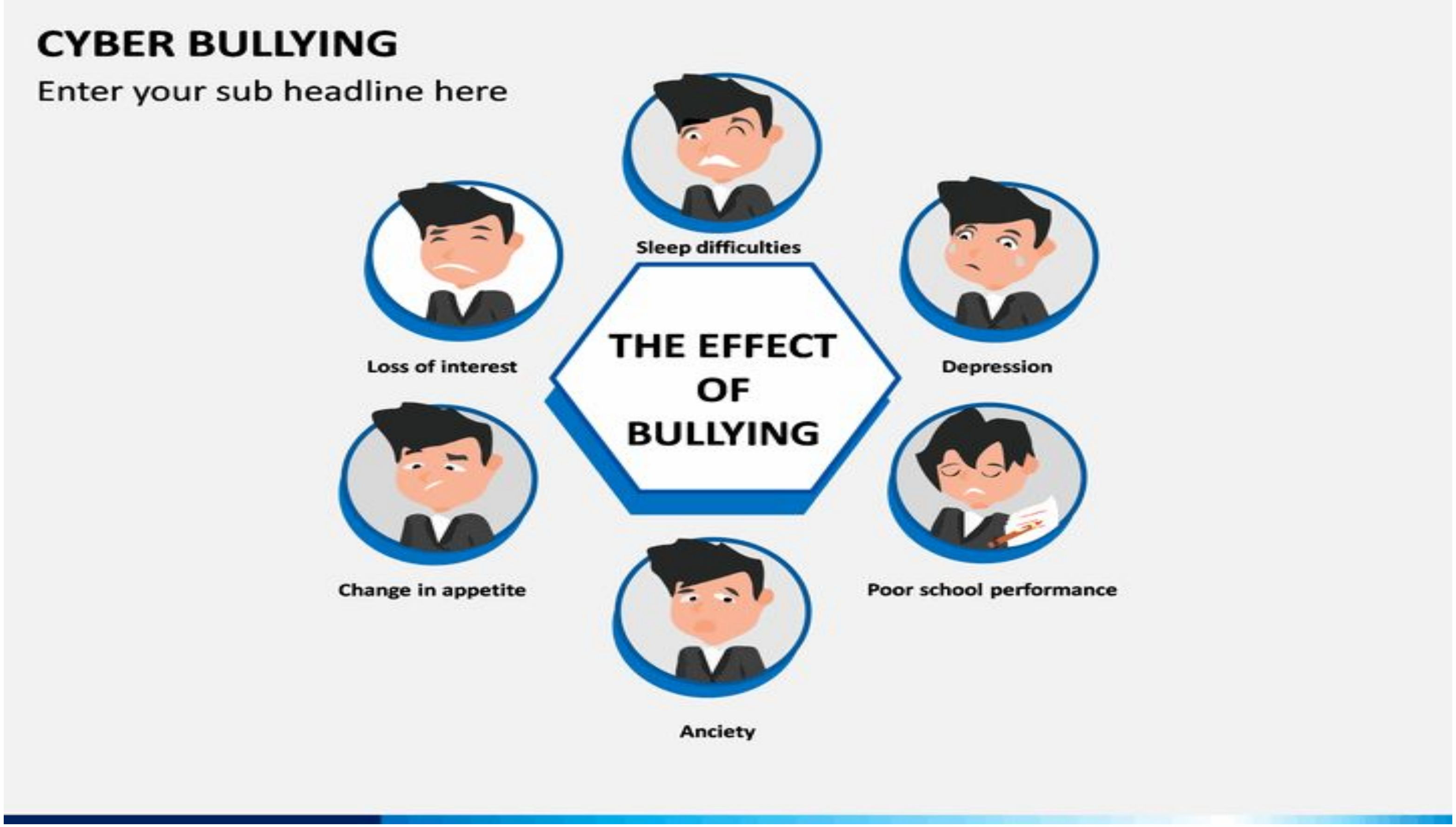
H, a twelve-year-old school boy was increasingly withdrawn and introverted. He looked worried most of the time but refused to divulge his troubles to his parents who were aware that he spent an extra-ordinary amount of after-school time on his I-Pad. One night, after H went to bed, his parents accessed his I-Pad and found that he was on various chat groups and was being bullied online by his classmates. The bullying involved name calling and derogatory remarks regarding his clothes and his grades.

In such scenario, the remedies available to H's parents are as following:

In such scenario, the remedies available to H's parents are as following:

- Take prompt steps to show support to H;
- File a complaint reporting the online bullying to the school authorities. The complaint shall be looked into by the Anti Bullying Committee required to be formed in every school in accordance with the ‘CBSE Guidelines for prevention of Bullying and Ragging in Schools';
- Report the online bullying to the nearest police station, who shall refer the matter to the cyber-crime cell for investigation. Thereafter, the cyber-crime cell shall report the matter to the Juvenile Justice Board, which will conduct an inquiry and deal with the incident as per the provisions of the Juvenile Justice (Care and Protection of Children) Act, 2000.

Effect of cyber bullying



CYBER BULLYING

Enter your sub headline here

THE EFFECT OF BULLYING

Sleep difficulties

Loss of interest

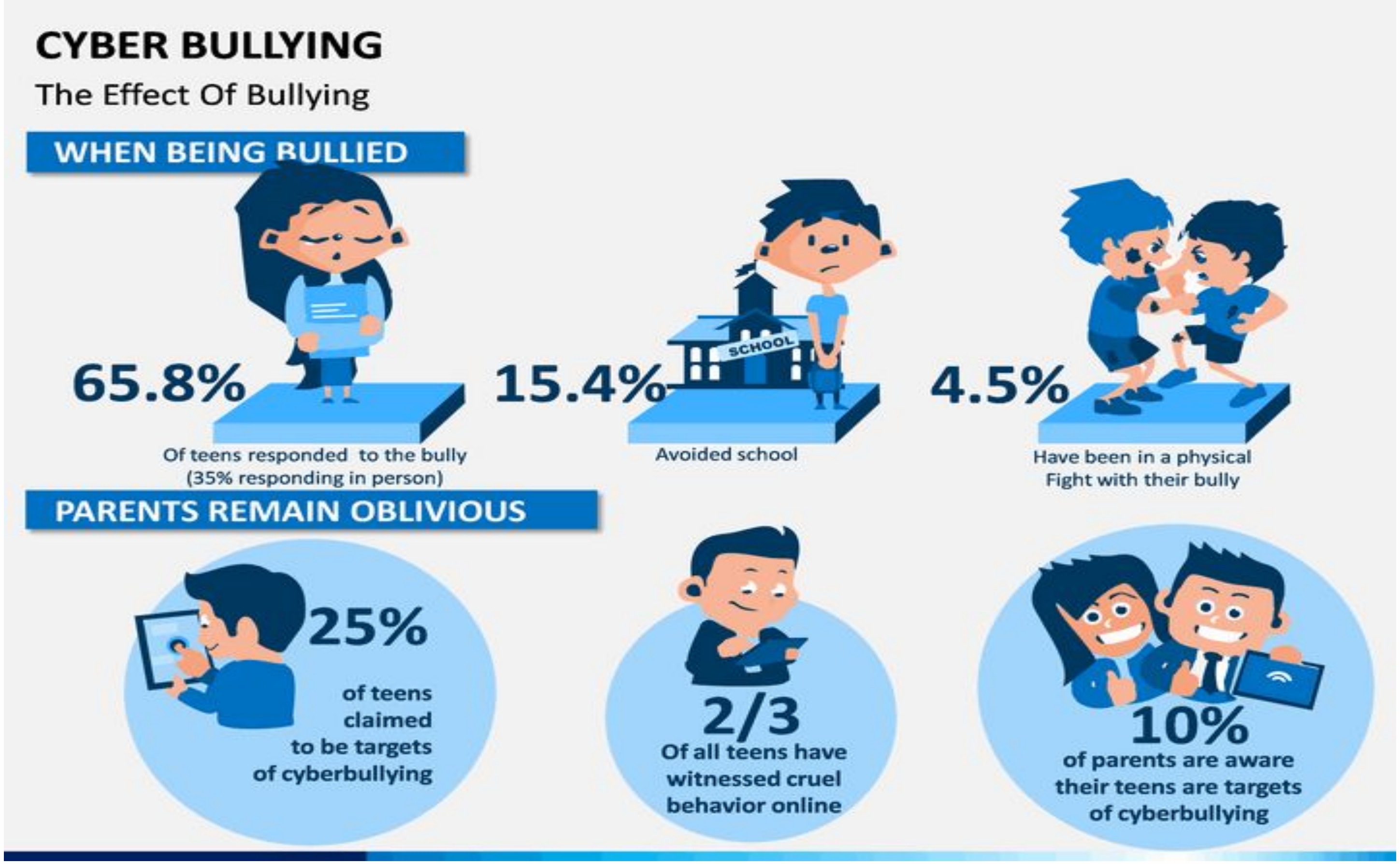
Depression

Change in appetite

Poor school performance

Anciety

Effect of cyber bullying



CYBER BULLYING

The Effect Of Bullying

WHEN BEING BULLIED

65.8% Of teens responded to the bully (35% responding in person)

15.4% Avoided school

4.5% Have been in a physical Fight with their bully

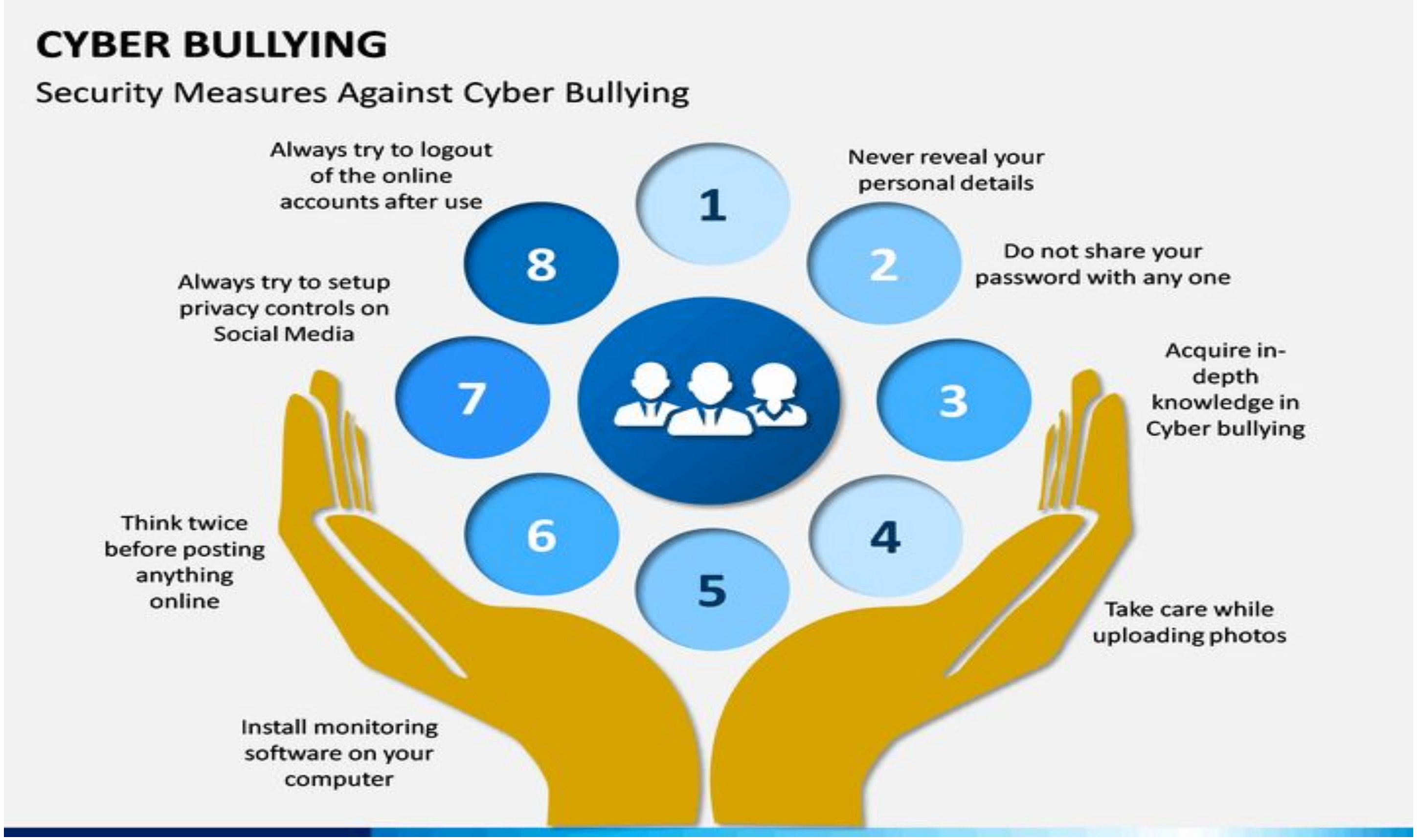
PARENTS REMAIN OBLIVIOUS

25% of teens claimed to be targets of cyberbullying

2/3 Of all teens have witnessed cruel behavior online

10% of parents are aware their teens are targets of cyberbullying

Prevention

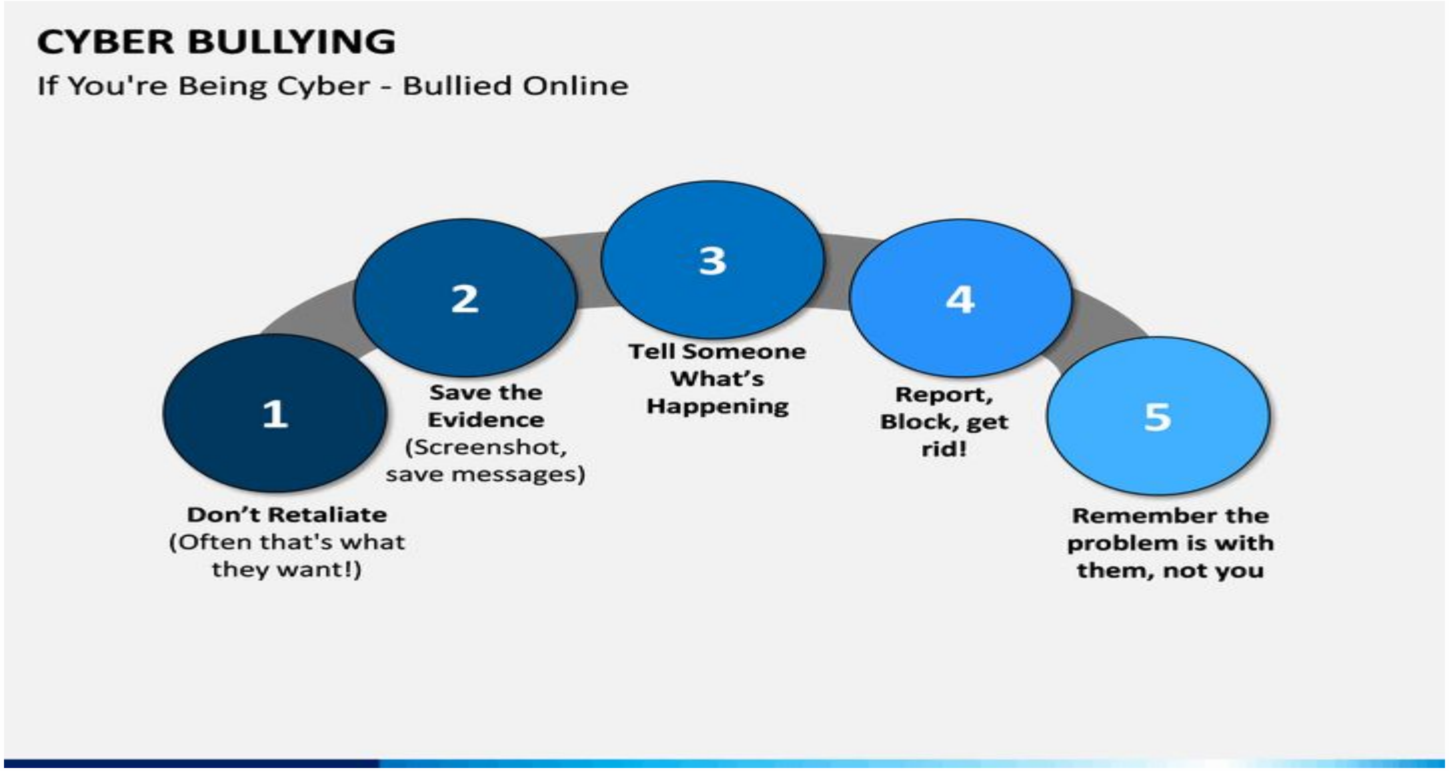


CYBER BULLYING

Security Measures Against Cyber Bullying

1. Never reveal your personal details
2. Do not share your password with any one
3. Acquire in-depth knowledge in Cyber bullying
4. Take care while uploading photos
5. Install monitoring software on your computer
6. Think twice before posting anything online
7. Always try to setup privacy controls on Social Media
8. Always try to logout of the online accounts after use

Conclusion



CYBER BULLYING

If You're Being Cyber - Bullied Online

1 Don’t Retaliate (Often that's what they want!)

2 Save the Evidence (Screenshot, save messages)

3 Tell Someone What’s Happening

4 Report, Block, get rid!

5 Remember the problem is with them, not you

Warning sign of cyber bullying

https://cyberbullying.org/cyberbullying-warning-signs.pdf

Cyber Security Laws in India

- **Information Technology Act (2000):** Enacted by the parliament of India, the information technology act was made to safeguard the e-governance, e-banking, and e-commerce sectors; but now, its scope has been enhanced to encompass all the latest communication devices.

- **Indian Penal Code (IPC) (1980):** This cybercrime prevention act has primary relevance to cyber frauds concerning identity theft and other sensitive information theft.

- **Companies Act (2013):** With the companies act enacted back in 2013, the legislature ensured that all the regulatory compliances are covered, including e-discovery, cyber forensics, and cybersecurity diligence. The Companies Act provides guidelines for the responsibilities of the company directors and leaders concerning confirming cybersecurity obligations.

- **NIST Compliance:** The Cybersecurity Framework (NCFS), authorized by the National Institute of Standards and Technology (NIST), contains all the guidelines, standards, and best practices necessary to responsibly address cybersecurity risks.

Cyber Security Laws in India

Offence under IT Act	*Relevant Section*
Tampering with Computer source documents	Sec.65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

Section 65: Source Code

- Most important asset of software companies
- “Computer Source Code" means the listing of programmes, computer commands, design and layout
- **Ingredients**

  Knowledge or intention
  Concealment, destruction, alteration
  computer source code required to be kept or maintained by law
- **Punishment**
- imprisonment up to three years and / or
- fine up to Rs. 2 lakh

Section 66: Hacking

- **Ingredients**
  - □ **Intention or Knowledge to cause wrongful loss or damage to the public or any person**
  - □ **Destruction, deletion, alteration, diminishing value or utility or injuriously affecting information residing in a computer resource**
- **Punishment**
  - □ **imprisonment up to three years, and / or**
  - □ **fine up to Rs. 2 lakh**
- **Cognizable, Non Bailable,**
- *Section 66 covers data theft aswell as data alteration*

Sec. 67. Pornography

- **Ingredients**
  - Publishing or transmitting or causing to be published
  - in the electronic form,
  - Obscene material
- **Punishment**
  - On first conviction
    - imprisonment of either description up to five years and
    - fine up to Rs. 1 lakh
  - On subsequent conviction
    - imprisonment of either description up to ten years and
    - fine up to Rs. 2 lakh
- **Section covers**
  - Internet Service Providers,
  - Search engines,
  - Pornographic websites

Computer Related Crimes under IPC and Special Laws

Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499, 500 IPC
Forgery of electronic records	Sec 463, 470, 471 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 416, 417, 463 IPC
Online sale of Drugs	NDPS Act
Web - Jacking	Sec. 383 IPC
Online sale of Arms	Arms Act

References

1. https://www.knowledgehut.com/blog/security/cyber-security-laws#what-is-cyber%C2%A0law?%C2%A0
2. https://www.cybersmile.org/advice-help/category/what-is-cyberbullying
3. https://blog.ipleaders.in/cyber-law-ethics-india/

DIGITAL LEARNING CONTENT