Fundamentals of Information Security

Prepared By : Jayshree Dasa

Unit - 2

Exploring Ethics as it Relates to Cybersecurity

Prepared By : Jayshree Dasa

ETHICS and LAW

What Is a Law?

Law for business consists of a set of required norms of behavior. The essence of law is that it commands behavior under threat of punishment or sanction.

What Is Ethics?

- Ethics is the study of man as moral being, one who is rationally able to distinguish between right and wrong.

What is the difference between Law and Ethics?

- Laws are a set of rules and regulations enforced by the government or authorities while ethics are morals and principles adapted by society from the environment.

- Failure to follow laws can result in penalties and punishment while ethics do not attract penalties and punishment.

CONTRACTS AND ETHICS

- The very process of business is making and fulfilling contracts. Without contracts, no business would be possible.

WARRANTY

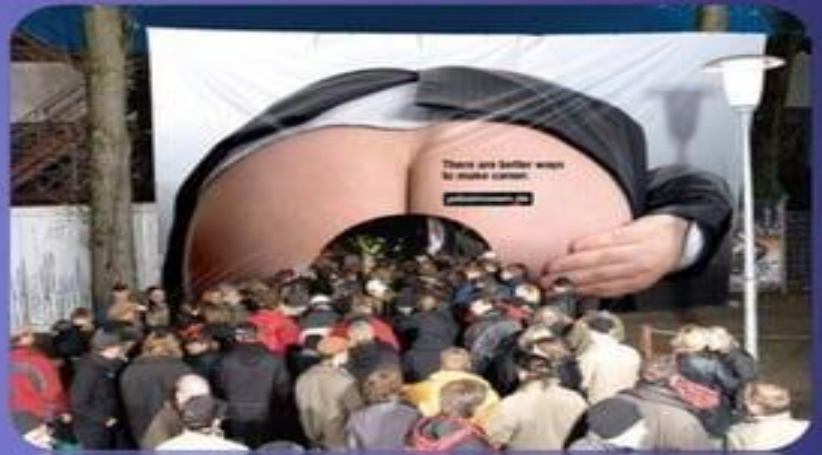
WARRANTY

- It is essentially a binding promise that the product is fit for its intended purposes, is free of defects and works

ADVERTISING

FALSE ADVERTISING

- It is against the law



- It is unethical


EMPLOYMENT LAW


EMPLOYMENT
LAW RIGHTS

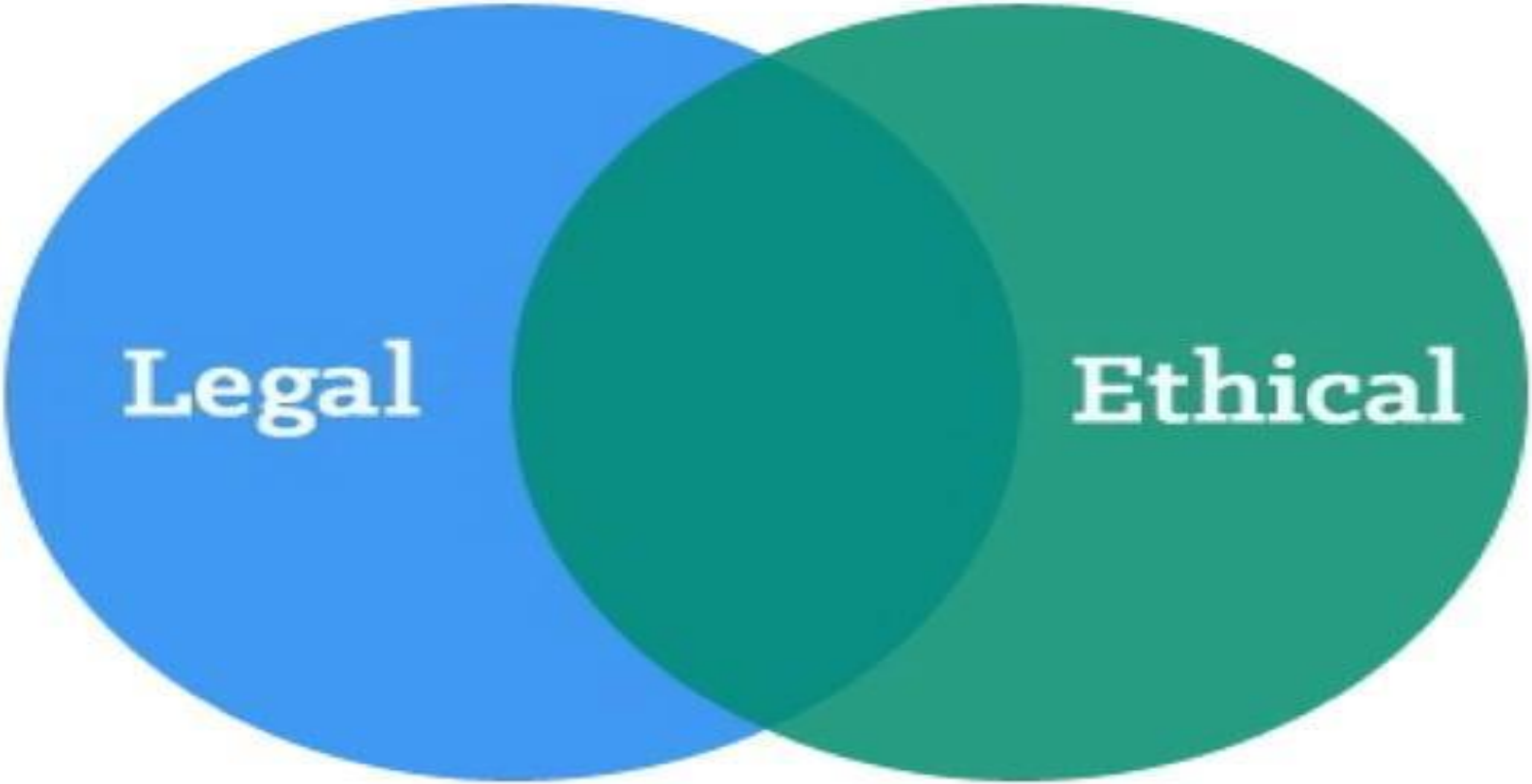
❖ EMPLOYMENT-AT-WILL

❖EMPLOYMENT DISCRIMINATION LAW

HOW ARE LAW AND ETHICS RELATED?

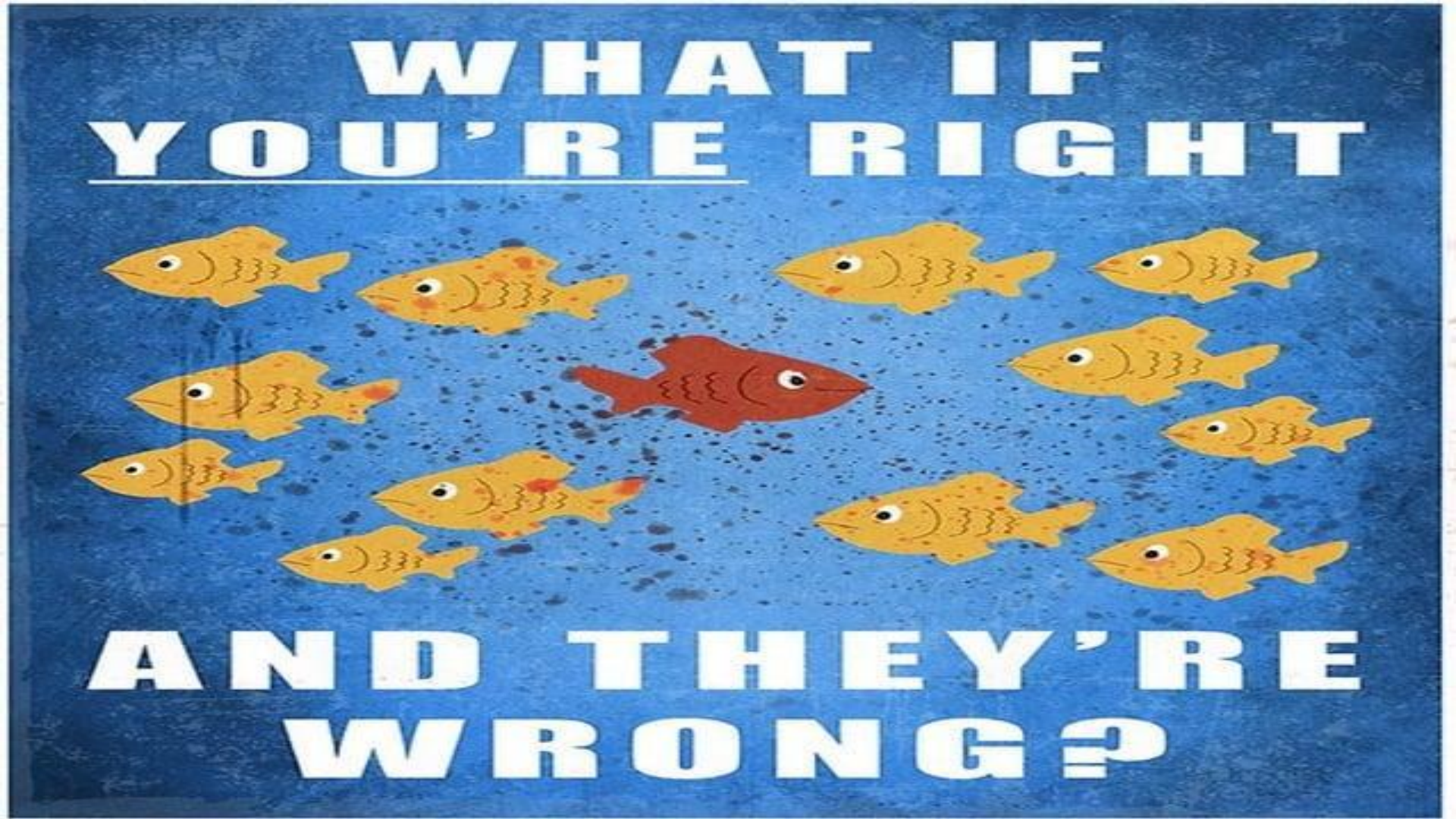
Ethics and Law

- Ethical rules are necessary
- Legality is not identical with morality
- sometimes, what is moral is not always legal
- ethics includes thoughts and feelings
- private actions is also under ethics


Legal
Ethical

Ethics and Law

- things we do that dont harm others or even to ourselves
- things we do that harm others or us on later part
- Laws are product of Collective Agreement
- Morality is not based on how many people agreed is its good or bad


WHAT IF
YOU'RE RIGHT
AND THEY'RE
WRONG?

WRONG IS WRONG

even if everyone is doing it.

RIGHT IS RIGHT

even if no one is doing it.

Ethics and Law

- Lastly, we still need ethics even if we laws because ethics serves as FOUNDATION OF LAWS.

- Therefore, Morality Precedes Legality for its Scopes and Implications are Deeper and Wider

Ethics
is
Prescriptive

Ethics

key terms:

- should
- should not
- must
- must not
- just
- unjust
- duty
- obligation

What does Ethics tell us?

- what we ought TO DO AND NOT TO DO
- PURSUE the good things
- REFRAIN evil doings

Computer Ethics	Is a system of moral standards or moral values used as a guideline for computer users
Code of Ethics	Is a guideline in ICT that help determine whether a specific computer action is ethical or unethical
Intellectual Property	Is works created by inventors, authors and artists
Privacy	Refers to the right of individuals and companies to deny or restrict the collection and use of information about them
Computer Crime	Is any illegal acts involving computers
Cyber Law	Is any laws relating to protect the Internet and other online communication technologies

ETHICS	LAW
As a guideline to computer users	**As a rule** to control computer users
Computers users are **free to follow** or ignore the code of ethics	Computers users **must follow** the regulations and law
Universal, can be applied anywhere, all over the world	**Depend on country** and state where the crime is committed
To produced **ethical** computers users	To prevent **misuse** of computers
Not following ethics are called **immoral**	Not obeying laws are called **crime**

Difference between IPC and IT Act.

Aspect	Information Technology Act, 2000 (IT Act)	Indian Penal Code (IPC)
Purpose	Focuses on cybercrimes and electronic transactions.	Covers general criminal offenses across various areas.
Scope	Specific to cyber-related issues (e.g., hacking, data theft).	Broad range of criminal activities (e.g., theft, fraud).
Key Sections	- Section 43: Damage to computer systems - Section 66: Computer-related offenses - Section 66C: Identity theft - Section 66D: Cheating by personation - Section 66F: Cyber terrorism - Section 65: Tampering with source code - Section 69: Monitoring of communications	- Section 403: Misappropriation of property - Section 405: Criminal breach of trust - Section 415: Cheating - Section 469: Forgery - Section 500: Defamation

Aspect	Information Technology Act, 2000 (IT Act)	Indian Penal Code (IPC)
Penalties	Includes fines, imprisonment (up to life for severe offenses).	Varies by offense; includes fines and imprisonment.
Focus	Specialized in digital crimes and electronic data.	General criminal code applicable to various types of crimes.
Application	Directly addresses cybercrimes and e-commerce issues.	Applies to a wide range of criminal activities, including some related to cyber issues.

IT ACT 2000

Introduction

- This is the primary law in India dealing with **Cyber crimes & Electronic Commerce**
- It was commenced on **17th October 2000**
- There are total **94** Sectors, **13** Chapters, and **4** schedules
- Amendment – IT Amendment Act, 2008

What is IT Act?

- The IT Act (Information Technology Act, 2000) in the context of cyber security is a law that provides the legal framework to address issues related to online activities, digital communication, and cybercrimes.
- It defines various cybercrimes, such as hacking, data theft, and unauthorized access, and prescribes penalties for these offenses.
- The act also ensures the protection of electronic data, legal recognition of electronic documents, and secure electronic transactions, thereby safeguarding individuals and businesses in the digital world.

Section 43

Section 43: Penalty and Compensation for damage to computer, computer system, etc.

Provision: This section deals with unauthorized access to computers, downloading, copying, or extracting any data, or damaging the system.

Example: If someone hacks into another person's computer and deletes files, they can be penalized under this section.

Penalty/Punishment: The person responsible for unauthorized access, downloading, copying, or causing damage to a computer system may be liable to pay damages by way of compensation to the affected party. The compensation can go up to ₹1 crore (10 million rupees).

Section 65

Section 65: Addresses tampering with computer source documents.

Example: Modifying or concealing computer source code without authorization, like altering software code in a way that causes harm.

Penalty/Punishment:

Imprisonment: Up to 3 years.

Fine: May extend up to ₹2 lakh (200,000 rupees), or both.

Section 66

Section 66: Computer-related offenses.

Provision: This section includes various computer-related offenses such as identity theft, sending offensive messages through communication services, cheating by personation, and more.

Example: If someone creates a fake email ID and sends out defamatory or harmful messages, they can be prosecuted under Section 66.

Penalty/Punishment: Any person found guilty under this section can face imprisonment for up to 3 years and/or a fine that may extend up to ₹5 lakh (500,000 rupees).

Section 66A

Section 66A: Sending Offensive Messages through Communication Services

Provision: This section dealt with punishing anyone who sent offensive or menacing messages through electronic communication.

Example: Sending abusive or threatening messages to someone via email or social media.

Penalty/Punishment: The punishment included imprisonment for up to 3 years and fine.

Section 66C: Identity theft.

Section 66C: Identity theft.

Provision: It addresses the use of someone's identity (e.g., passwords, digital signatures) without their permission.

Example: Using another person's digital signature to authorize a transaction would be punishable under this section.

Penalty/Punishment: The punishment for identity theft under this section includes imprisonment for up to 3 years and/or a fine that may extend up to ₹1 lakh (100,000 rupees).

Section 66D

Section 66D: Cheating by personation by using computer resources.

Provision: It penalizes anyone who cheats by pretending to be someone else using a computer resource.

Example: Phishing attacks where someone poses as a legitimate entity to steal sensitive information fall under this section.

Penalty/Punishment: The offense under this section is punishable with imprisonment for up to 3 years and/or a fine that may extend up to ₹1 lakh (100,000 rupees).

Section 66E

Section 66E: Violation of Privacy

Provision: This section penalizes the capturing, publishing, or transmitting of the image of a private area of any person without their consent, in a manner that violates their privacy.

Example: Secretly taking photos of someone in a changing room and sharing them online without their permission.

Penalty/Punishment: Imprisonment for up to 3 years and/or a fine not exceeding ₹2 lakh (200,000 rupees).

Section 66F

Section 66F: Cyber Terrorism

Provision: This section addresses cyber terrorism, which involves any act using computers or communication networks that threatens the sovereignty, integrity, or security of India, or creates fear or panic among the public.

Example: Launching a cyberattack on critical infrastructure like power grids or defense systems, causing widespread disruption and panic.

Penalty/Punishment: Imprisonment for life.

IPC Sections

Section 403

Section 403: Misappropriation of Property

Provision: This section deals with the dishonest misappropriation or conversion of property for one's own use.

Example: Taking data or digital assets from a company and using them for personal gain without authorization.

Penalty/Punishment: Imprisonment for up to 2 years, or a fine, or both.

Section 405

Section 405: Criminal Breach of Trust

Provision: This section addresses the criminal breach of trust, where a person entrusted with property dishonestly misappropriated it.

Example: An employee who is given access to confidential data and uses it for unauthorized purposes or discloses it improperly.

Penalty/Punishment: Imprisonment for up to 3 years, or a fine, or both.

Section 415

Section 415: Cheating

Provision: This section covers cheating by deceiving someone to gain an advantage or cause harm.

Example: Creating a fake online store to defraud people of their money.

Penalty/Punishment: Imprisonment for up to 1 year, or a fine, or both.

Section 469

Section 469: Forgery

Provision: This section deals with forgery intended to harm someone's reputation or cause a legal disadvantage.

Example: Forging digital documents or signatures to commit fraud.

Penalty/Punishment: Imprisonment for up to 3 years, or a fine, or both.

Section 500

Section 500: Defamation

Provision: This section pertains to defamation, which involves harming a person's reputation through false statements.

Example: Posting false and damaging information about someone online.

Penalty/Punishment: Imprisonment for up to 2 years, or a fine, or both.

Victoria County Community Access Program Society

CYBER BULLYING

WHAT IS CYBER BULLYING?

Bullying is generally understood as an aggressive and intentional act or behaviour carried out by a group or an individual repeatedly and over time against a victim who cannot easily defend him or herself.

The term **cyberbullying** is used to describe bullying taking place on the internet mostly through mobile phones and social media.

WHY IS IT SO IMPORTANT?

- 1/3 children has been a victim of cyber-bullying.
- Nearly half of suicides among 10 to 14-year-olds are due to bullying.
- 1 in 7 teachers is a victim of cyber-bullying.

Elements characterizing cyberbullying

- The use of electronic or digital means
- Intentional harm
- Imbalance of power
- Repetition
- Sense of anonymity and lack of accountability
- Publicity

- Cyber bullies often also become victims of cyber bullying. People frequently change roles when it comes to cyber bullying.

- It can only be limited by a child's imagination or their access to cyber technology.

There are two kinds of Cyber Bullying…

- Direct Attacks- messages sent directly to the victim.
- Cyber Bullying by Proxy- Using someone else to cyber bully a victim, this proxy may know they are cyber bullying and they may not.

Direct Attacks…

- Instant Messaging
- Text Messaging
- Blogs
- Websites
- Emailing Pictures
- Stealing Passwords
- Internet Polling- Hot or Not!
- Hacking or sending spyware

By Proxy…

- Someone else does the dirty work for the main cyber bully.
- Bullies may hack into the victim's account or steal their password. They may set up a new account pretending to be the victim.
- Friends get angry with the victim.
- This form of cyber bullying is very dangerous because many people are involved, not just the bully and the victim.

MEANS USED

- Cyberbullying can be carried out through different means, such as mobile devices, internet, messaging (e.g. instant messaging, chat programs, text/audio/video programs, multimedia messages, gaming devices and social networks).
- Initial research in this area showed that the most common channels to perpetrate cyberbullying were phone calls and text messages.
- However, the rapid pace of ICT innovation determined changes in patterns. Nowadays, cyberbullying is increasingly performed through social networks (mostly Facebook, followed by Twitter, Instagram, Tumblr and YouTube)

VICTIMS

- Trends reflect a relationship between age and frequency of victimization with a higher number of victims in the group of 13–15-year-old children.
- According to the Net Children Go Mobile survey, which interviewed 3,500 children of seven EU Member States, over the period 2013–2014, children between 13 and 14 years of age were the most affected by cyberbullying.
- Victims of cyberbullying tend to be younger than the perpetrators.
- More than twice the number of teenage girls being cyberbullied compared to boys.

Why do children Cyber Bully?

- Anger
- Frustration
- Revenge
- Entertainment
- To get Laughs or Reactions
- Power Hungry
- Because all motives for bullying are different so are the solutions and responses.

Who Does This Affect?

- As hinted at previously, Cyber Bullying only impacts children.
- Children of all ages can be victims of cyber bullying, Young children, Preteens and Teenagers.
- Once adults get involved with Cyber Bullying it becomes Cyber Stalking or Cyber Harassment.

Consequences of Cyber Bullying

- Anxiety
- Depression
- Stress Related Disorders
- Suicide
- Withdrawal from Friends and Activities
- Changes in mood, behaviour and appetite
- Emotional Distress during and after using technology

http://kidshealth.org/parent/positive/talk/cyberbullying.html#

FORMS OF CYBERBULLYING

Behavior	Definition
Exclusion	the rejection of a person from an online group provoking his/her social marginalization and exclusion
Online harassment	the repetition of harassment behaviours on the net, including insults, mocking, slander, menacing chain messages, denigrations, name calling, gossiping, abusive or hate-related behaviours. Harassment differs from nuisance in light of its frequency. It can also be featured as sexual harassment if it includes the spreading of sexual rumours, or the commenting of the body, appearance, sex, gender of an individual.
Griefing	the harassment of someone in a cyber-game or virtual word (e.g. ChatRoulette, Formspring, etc.)
Flaming	the online sending of violent or vulgar messages. It differentiates from harassment on the basis that flaming is an online fight featured by anger and violence (e.g. use of capital letter or images to make their point)
Trolling	the persistent abusive comments on a website

FORMS OF CYBERBULLYING

Behavior	Definition
Cyberstalking	involves continual threatening and sending of rude messages.
Cyber - persecution	continuous and repetitive harassment, denigration, insulting, and threats.
Masquerade	a situation where a bully creates a fake identity to harass someone else.
Impersonation	the impersonation of someone else to send malicious messages, as well as the breaking into someone's account to send messages, or like posts that will cause embarrassment or damage to the person's reputation and affect his/her social Life.

Cyberbullying -VS- Bullying

Bullying	Cyberbullying
Face – to - face	24 hours a day, 7 days a week, 365 days/yr
Can find a safe space or escape	No safe space – hard to escape
Limited to onlookers	Shared by wide audience – can go viral in a matter of seconds
Bully can be identified	Bully can be anonymous
Can see facial and body reaction of target and onlookers	Harder to empathize with the target
	No geographical limitations
	The target can easily become the bully

Bullying online and offline seem also to be linked. Cyberbullying perpetrators are often involved as victims or perpetrators in traditional bullying.

Why is Cyberbullying so hurtful?

1. **Permanence:** The insults, comments or images can be preserved by the person who was bullied or by others so that the victim may read or view them over and over again and the harm is re-inflicted with each reading or viewing.

Why is Cyberbullying so hurtful?

2. **Audience size:** The size of the audience that is able to view or access the damaging material increases the victim's humiliation.

Why is Cyberbullying so hurtful?

3. **Familiarity:** many young people are friends with or know their cyber bully either threw school or other personal connections, increasing the potential for embarrassment and humiliation.

Why is Cyberbullying so hurtful?

4. Social Networking: Social Networking sites such as Facebook and MySpace allow cyber bullies to engage in campaigns against a particular person which may involve many others.

Why is Cyberbullying so hurtful?

5. **Speed:** The speed at which harmful messages can reach large audiences also plays a major part in making cyberbullying so damaging to the targets.

How to help prevent cyberbullying?

- Block all communication with cyberbullies
- Do not forward any messages, comments, etc. that involve cyberbulling
- Always report any cyberbulling taking place to an adult

Tips How to Stop a Cyberbully

- Be private - keep passwords, pictures and secrets to yourself.
- Take five - don't reply in anger.
- Stop, block and tell - don't reply, block the sender, tell someone.
- Save the evidence - on your computer or print out.
- Google yourself.

Steps to Take if you believe you have been a victim of Cyberbullying

- Determine if cyberbullying is actually going on.
- Save the evidence.
- Identify the sender - contact your ISP (Internet Service Provider) if necessary.
- Contact the offender's parents - who may or may not be supportive.
- Back up your remarks with written evidence.
- Contact your school.
- Threats, extortion, sexual harassment should be reported to the police.

How you can help!

- Don’t engage in or support mean material,gossip, or rumors posted online, or talk about it.
- Support the victim being targeted online byposting positive messages!
- Print the evidence to share with an authority.

Remember!

We are not invisible online, and anything we post can be traced back to us.

Monitor your online reputation!

Prevention

- Education of students is the best way to teach children about the seriousness of cyber bullying.
- Schools can take action with discipline for IN-SCHOOL situations only.
- Teach students techniques for calming down so they do not react with anger and revenge using technology.

Resources

- http://cyberbullying.novascotia.ca/ This website has great information for parents, teachers, and students.
- http://www.stopcyberbullying.org/index2.htm Information for all ages.
- http://www.bewebaware.ca/english/cyberbull

- If you are being cyber bullied, or you know someone who is you can also call the Kids Help Phone at 1-800-668-6868

https://www.slideshare.net/slideshow/cyber-security-and-cyber-laws/242012700

Thank you