CYBER ETHICS

Ethics is a branch of philosophy concerned with how people should act in a general sense or in a specific circumstance. In philosophy ethics is very important because most philosophers regardless of their particular focus have at least something to say about ethics and that something is often a very big clue as to what that philosopher is all about. Ethics is where terms such as right and wrong or good and evil get their meaning. Applied ethics, unlike theoretical ethics, examines "practical" ethical issues. In the present time, we all are connected to the internet and pass a lot of time in cyber world. So, we have to follow some manner to interact with other individuals in internet. So, cyber ethics was introduced and now it is considered as a part of Applied Ethics.

Cyber ethics:

"Cyber ethics" refers to the code of responsible behavior on the Internet. Just as we are taught to act responsibly in everyday life with lessons such as "Don't take what doesn't belong to you" and "Do not harm others," we must act responsibly in the cyber world as well. The basic rule is "Do not do something in cyberspace that you would consider wrong or illegal in everyday life."

Considerations When Determining Responsible Behavior:

1. Do not use rude or offensive language.
2. Do not cyber bully.
3. Do not plagiarize.
4. Do not break into someone else's computer.
5. Do not use someone else's password.
6. Do not attempt to infect or in any way try to make someone else's computer unusable.
7. Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.

The main issues that surround cyber ethics are: Copyright/Downloading, Hacking and cyber bullying. These issues are increasing daily and mos- tly due to children using the internet improperly.

Copyright/Downloading:

This has become a major problem due to programs like Napster and Lim- eWire which allow users to download music, programs and videos for free. Many people, especially children, do not realize that thisbeh- avior has major consequences.

A copyright is a right granted by the state that allows an author to have exclusive control over a work for a limited amount of time in exchange for public disclosure of the work. In the U.S., copyrights are granted by the U.S. Copyright office. Although a copyright vests in the author as soon as her creation is fixed in a tangible medium, there are additional benefits to filing for copyright registration with the U.S. Copyright office.

Copyright infringement occurs when an author's rights are violated because their work is reproduced, distributed, performed, publicly displayed or made into a derivative work without their consent. When you download a copy of a copyrighted work without the permission of the owner, you are essentially reproducing that work and engaging in copyright infringement.

If you violate copyright law by downloading copyrighted material with- out the author's consent, you could potentially face a lawsuit for copyright infringement. U.S. copyright law states that violators can be responsible for paying the other party's attorney's fees as well as anywhere between $750 and $30,000 for each violation. U.S. law also allows for criminal penalties for severe violations.

Generally, most authors do not sue individuals downloading their materials illegally over the web. However, large artist organizations such as the RIAA and the MPAA routinely bring copyright infringement lawsuits in attempts to dissuade the public from downloading copyrighted material and violating copyright laws. If you are not sure if the material you are downloading is authorized for free download, check to see if the author has a website or a statement about their works anywhere on the Internet.

Hacking:

Hacking is the intentional damage that a person inflicts onto another computer or computer network. This can include stealing classified information, stealing passwords to get into a site and also changing 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. Cybercitizenship.org gives a chilling example: "If a virus were to disable the computer network of a hospital, it could shut down medical instrumentation systems that control life support and monitoring functions-all of which could cost a patient his or her life." Children need to be aware of this extreme consequences.

Hacking generally refers to unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.

Many victims of hacking are ashamed to come forward due to the limited resources available to them. One of the worst feelings in the digital age is when someone falls victim to a breach of their privacy. Being hacked can cause great stress and humiliation to those on the wrong side of the attack, leaving them feeling powerless and totally duped. Most shameful fact is sometimes hackers leak personal image of victim on internet. This often happened to celebrity. Recently, Jennifer Lawrence’s naked image was exposed and she commented on the hack, she felt sexually violated.

Hacking in INDIA:

There have been numerous hacking attacks on Indian government websites where state government websites or defense websites have been hacked. Some time back, the Principal Comptroller of defense accounts website was hacked due to which defense officials could not access their salary information. The government, to reduce hacking of precise work, has agreed to the proposal of DEITY, which is the department of information and technology to stop using popular email ids for official purpose and has sanctioned a budget of Rs. 100 cores to safeguard the data. The websites of state governments have also been hacked in the past. The official website of Maharashtra government was hacked, and the hackers were not traceable. There have been some professional hackers in India who have taken huge amounts to hack data from websites. In the infamous case of Amit Tiwari, who was a global hacker, he has hacked more than 950 accounts since 2003 and was caught by the police only in 2014. This shows the lack of evidence and the difficulty in arresting a hacker.

To prevent this situation Indian government has applied many laws on hacking. Section 43 and section 66 of the IT Act cover the civil and criminal offenses of data theft or hacking respectively. Under section 43, a simple civil offense where a person without permission of the owner accesses the computer and extracts any data or damages the data contained therein will come under civil liability. The cracker shall be liable to pay compensation to the affected people. Under the ITA 2000, the maximum cap for compensation was fine at Rs. One crore. However in the amendment made in 2008, this ceiling was removed. Section 43A was added in the amendment in 2008 to include corporate shed where the employees stole information from the secret files of the company. Section 66B covers punishment for receiving stolen computer resource or information. The punishment includes imprisonment for one year or a fine of rupees one lak or both. Men rea is an important ingredient under section 66A. Intention or the knowledge to cause wrongful loss to others i.e. the existence of criminal intention and the evil mind i.e. concept of men rea, destruction, deletion, alteration or diminishing in value or utility of data are all the major ingredients to bring any act under this Section. The jurisdiction of the case in cyber laws is mostly disputed. Cybercrime does not happen in a particular territory. It is geography less and borderless. So it gets very difficult to determine the jurisdiction under which the case has to be filed. Suppose a person works from multiple places and his data gets stolen from a city while he resides in some other city, there will be a dispute as to where the complaint should be filed.

Law against Hacking in Bangladesh:

In Bangladesh, a draft Bill on Information and Communication Technology has been introduced in the Parliament. The final report on the Law on Information Technology was approved by the Office of the Law Commission in its meeting dated 08.09.2002.

The Proposal: Chapter VII on Penalties and Adjudication and Chapter IX on Offences includes some cybercrime provisions that prohibits attacks or unauthorized access to computers and computer systems.

Chapter IX: Section 66. Punishment for tampering with computer source documents

Whoever intentionally or knowingly conceals, destroys or alters or intentionally or knowingly causes any other person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by any law for the time being in force, shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two lakhs, or with both. Explanation. For the purpose of this section, “computer source code” means the listing of programs, computer commands, design and layout and program analysis of computer resource in any form.

Section 67. Hacking with computer system

Whoever, with the intent to cause or knowing that he is likely to cause wrongful loss or damages to the public or any other person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits the offence of “hacking”.

Section 68. Punishment for hacking

Whoever commits hacking shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two laks, or with both.

Cyber bullying:

Bullying does not only happen in real life anymore. Cyber bullying is growing and people are becoming aware of its effect on children. Cyber bullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyber bullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyber bullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyber bullying crosses the line into unlawful or criminal behavior.

The most common places where cyberbullying occurs are:

1. Social Media, such as Facebook, Instagram, Snapchat, and Twitter
2. SMS (Short Message Service) also known as Text Message sent through devices
3. Instant Message (via devices, email provider services, apps, and social media messaging features)
4. Email

With the prevalence of social media and digital forums, comments, photos, posts, and content shared by individuals can often be viewed by strangers as well as acquaintances. The content an individual share online – both their personal content as well as any negative, mean, or hurtful content – creates a kind of permanent public record of their views, activities, and behavior. This public record can be thought of as an online reputation, which may be accessible to schools, employers, colleges, clubs, and others who may be researching an individual now or in the future. Cyber bullying can harm the online reputations of everyone involved – not just the person being bullied, but those doing the bullying or participating in it. Cyber bullying has unique concerns in that it can be:

Persistent – Digital devices offer an ability to immediately and continuously communicate 24 hours a day, so it can be difficult for children experiencing cyber bullying to find relief.

Permanent – Most information communicated electronically is permanent and public, if not reported and removed. A negative online reputation, including for those who bully, can impact college admissions, employment, and other areas of life.

Hard to Notice – Because teachers and parents may not overhear or see cyber bullying taking place, it is harder to recognize.

Consequences of Cyberbullying

Sometimes, online bullying, like other kinds of bullying, can lead to serious long-lasting problems. The stress of being in a constant state of upset or fear can lead to problems with mood, energy level, sleep, and appetite. It also can make someone feel jumpy, anxious, or sad. If someone is already depressed or anxious, cyber bullying can make things much worse. It's not just the person being bullied who gets hurt. The punishment for cyber bullies can be serious. More and more schools and after-school programs are creating systems to respond to cyber bullying. Schools may dismiss bullies from sports teams or suspend them from school. Some types of cyber bullying may violate school codes or even break anti-discrimination or sexual harassment laws. So a bully may face serious legal trouble.

Why Do People Do It?

Why would someone be a cyberbully? There are probably as many reasons as there are bullies themselves. Sometimes, what seems like online harassment may be accidental. The impersonal nature of text messages, posts, and other ways of communicating online means it can be hard to figure out if someone is joking or not. Most people know when they're being bullied, though, because bullying involves repeated insults or threats. The people doing the bullying know they've crossed a line, too. It's not a one-off joke or insult — it's constant harassment and threats that go beyond typical fun teasing or a nasty comment made in anger.

What Should One Do About Cyber bullying?

Sometimes, people are afraid or not sure if they're being bullied or not. So they don't do anything about it. If you're being bullied, harassed, or teased in a hurtful way — or know someone who is — you don't have to suffer in silence. In fact, you absolutely should report any upsetting texts, messages, posts, or emails.

Tell someone. Most experts agree: The first thing to do is tell an adult you trust. This is often easier said than done. People who are cyber bullied may feel embarrassed or reluctant to report a bully. Some may hesitate because they're not 100% sure who is doing the bullying. But bullying can get worse, so speak up until you find someone to help. Sometimes the police can track down an anonymous online bully, so it's often worthwhile to report it. Most parents are so concerned about protecting their kids that sometimes they focus on taking major steps to stop the bullying. If you're being bullied and worry about losing your phone or computer privileges, explain your fears to your parents. Let them know how important it is to stay connected, and work with them to figure out a solution that doesn't leave you feeling punished as well as picked on. You may have to do some negotiating on safe phone or computer use — the most important thing is to first get the bullying under control. You also can talk to your school counselor or a trusted teacher or family member. If the bullying feels like it's really getting you down (like if it's affecting your sleep or concentration), therapy can help. If you're not ready for that, you can still benefit from the support of a trusted adult.

Walk away. What you've heard about walking away from a real-life bully works in the virtual world too. Ignoring bullies is the best way to take away their power, but it isn't always easy to do — in the real world or online.

Resist the urge to retaliate or respond. Walking away or taking a break when you're faced with online bullying gives you some space so you won't be tempted to fire back a response or engage with the bully or bullies. Responding when we're upset can make things worse. (Standing up to a bully can be effective sometimes, but it's more likely to provoke the person and escalate the situation.) Taking a break gives the power back to you!

Although it's not a good idea to respond to a bully, it is a good idea to save evidence of the bullying if you can. It can help you prove your case, if needed. You don't have to keep

mean emails, texts, or other communications where you see them all the time — you can ask a parent to make a copy or save them to a flash drive.

Report bullying. Social media sites take it seriously when people post cruel or mean stuff or set up fake accounts. If users report abuse, the site administrator may block the bully from using the site in the future. If someone sends you mean texts or emails, report it to phone service or email providers (such as Comcast, Google, and Verizon).

Block the bully. Most devices have settings that let you electronically block the bully or bullies from sending notes. If you don't know how to do this, ask a friend or adult who does.

Be safe online. Password protect your Smartphone and your online sites, and change your passwords often. Be sure to share your passwords only with your parent or guardian. It's also wise to think twice before sharing personal information or photos/videos that you don't want the world to see. Once you've posted a photo or message, it can be difficult or impossible to delete. So remind yourself to be cautious when posting photos or responding to someone's upsetting message.

If a Friend Is a Bully

If you know of a friend who is acting as a cyber bully, take him or her aside and talk about it. Without putting your friend down, stand up for your own principles: Let the bully know it's not OK.

Explain to your friend that bullying can have serious consequences: for the bully, for those being bullied, and even for bystanders like you and your friends.

Conclusion:

Use of technology by students is globally accepted as it facilitates the searching and retrieval of information needed for their academics and consequently the successful completion of their education programs. They need to be aware and knowledgeable about the ethics surrounding the use of ICT is therefore, important. Students must be aware and possess the knowledge about cyber ethics. Therefore, cyber ethics education must be provided to students by the school and college.

References:

1. https://en.wikipedia.org/wiki/Cyberethics

2. https://www.cisecurity.org/daily-tip/know-the-rules-of-cyber-ethics/

3. https://smallbusiness.chron.com/consequences-downloading-copyrighted-material-28212.html

4. https://blog.ipleaders.in/laws-hacking-india/

5. http://www.cybercrimelaw.net/Bangladesh.html

6. https://www.stopbullying.gov/cyberbullying/what-is-it/index.html

7. https://www.cbc.ca/news/canada/nova-scotia/anti-cyber-bullying-rally-takes-place-in-halifax-1.1042064