Cyber Ethics & Cyber Crime

**Cyberethics** is the philosophic study of ethics pertaining to computers, encompassing 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 defined policies about cyberethics. 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.

As the computer ethics was one of the major topics which had been studied in the past decades, in order to prevent the people from the social impact, in this part, authors provided a short review milestone on computer ethics and its historical enhancement.

In the mid 1970s, ‘**Walter Maner**’ began to use the term **cyber ethics** to refer to the field of inquiry dealing with ethical problems. He offered an experimental course on the subject at many universities. During the late 1970s, Maner generated computer ethics courses with varieties of workshops and lectures at computer science conferences and philosophy conferences across United States of America.

**In 1980s**, frequent numbers of social and ethical consequences of information technology were becoming public issues in the world, from computer-enabled crime, disasters caused by computer failures, invasions of privacy via computer databases to major law suits on software ownership. Because of the work of Parker and others, the foundation had been laid for computer ethics as an academic discipline.

**During the 1990s**, new university courses, research scholars, conferences, journals, articles and textbooks appeared, and a wide diversity of additional researchers and topics became involved. This era, generated new chapter of computer ethics with security in mind.

Accessibility, censorship and filtering bring up many ethical issues that have several branches in cyberethics. Many questions have arisen which continue to challenge our understanding of privacy, security and our participation in society. Throughout the centuries mechanisms have been constructed in the name of protection and security. Today the applications are in the form of software that filters domains and content so that they may not be easily accessed or obtained without elaborate circumvention or on a personal and business level through free or content-control software. Internet censorship and filtering are used to control or suppress the publishing or accessing of information. The legal issues are similar to offline censorship and filtering. The same arguments that apply to offline censorship and filtering apply to online censorship and filtering; whether people are better off with free access to information or should be protected from what is considered by a governing body as harmful, indecent or illicit. The fear of access by minors drives much of the concern and many online advocate groups have sprung up to raise awareness and of controlling the accessibility of minors to the internet.

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. It is especially hard to talk to teens because they do not want to be lectured about what is right and wrong. They seem to think they have it all sorts out. That is why is it is important to instill appropriate cyber etiquette at an early age but if you haven’t there is still time to tell to your child.

Cyber ethics concerns to the code of responsible behavior on the Internet. Just as we 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.

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

1. **Copyrighting or Downloading**
2. **Crime and Punishment**
3. **Internet Hacking**
4. **Cyberbullying**
5. **Copyrighting or Downloading:**

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.

1. **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.

1. **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.

1. **Cyberbullying:**

Cyberbullying is increasing and people are becoming aware of its effects on children. Cyberbullying is bullying that takes place carrying electronic technology. Electronic technology carried by devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, website and chat. When a child encounters cyber bullying that they should:

* Tell a trusted adult, and keep telling them until they take action.
* Avoid opening, reading or responding 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.

In this brief review it can be seen that many views of computer ethics exits. This richness of attitude is probably due to a difference in observation of computing characteristics, the adopted focus - broadly split between the outcome of computing or the undertaking of computing, and the disciplinary background. These perspectives can analyze computer ethics researched areas into several sub categories:

* Social - considering the computing-impact on society
* Professional - considering the manner of professional activity
* Universal activist - inclusive of communities around the globe
* Parochial - restricted consideration of current and future issues
* Ethics only - drawing only from ethics theory
* Multi-disciplinary - blending theory from several disciplines

### There are some other types of cyberethics exists. Like-

### Gambling:

Gambling is often a topic in ethical debate as some view it as inherently wrong and support prohibition or controls while others advocate no legal. "Between these extremes lies a multitude of opinions on what types of gambling the government should permit and where it should be allowed to take place. Discussion of gambling forces public policy makers to deal with issues as diverse as addiction, tribal rights, taxation, senior living, professional and college sports, organized crime, neurobiology, suicide, divorce, and religion." Due to its controversy, gambling is either banned or heavily controlled on local or national levels. The accessibility of the internet and its ability to cross geographic-borders have led to illegal online gambling, often offshore operations. Over the years online gambling, both legal and illegal, has grown exponentially which has led to difficulties in regulation. This enormous growth has even called into question by some the ethical place of gambling online.

**Sexuality and pornography:**

Sexuality in terms of sexual orientation, infidelity, sex with or between minors, public display and pornography has always stirred ethical controversy. These issues are reflected online to varying degrees. In terms of its resonance, the historical development of the online pornography industry and user-generated content have been the studied by media academics. One of the largest cyberethical debates is over the regulation, distribution and accessibility of pornography online. Hardcore pornographic material is generally controlled by governments with laws regarding how old one has to be to obtain it and what forms are acceptable or not. The availability of pornography online calls into question jurisdiction as well as brings up the problem of regulation in particular over child pornography, which is illegal in most countries, as well as pornography involving violence or animals, which is restricted within most countries.

Ethical issues can be involved into personal behavior and professional practice. Such as-

**Privacy:**

It may define as the claim of individuals to determine for themselves when, to whom, and to what extent individually identified data about them is communicated or used. Most invasions of privacy are not this dramatic or this visible. Rather, they creep up on us slowly as, for example, when a group of diverse files relating to a student and his or her activities are integrated into a single large database.

Collections of information reveal intimate details about a student and can thereby deprive the person of the opportunity to form certain professional and personal relationships. This is the ultimate cost of an invasion of privacy. So why integrate databases in the first place. It is because the bringing together of disparate data makes the development of new information relationships possible.

**Intellectual Property:**

One of the more controversial areas of computer ethics concerns the intellectual property rights connected with software ownership. Some people, like Richard Stallman who started the Free Software Foundation, believe that software ownership should not allow at all. He claims that all information should be free, and all programs should be available for copying, studying and modifying by anyone who wishes to do so. Others argue that software companies or programmers would not invest weeks and months of work and significant funds in the development of software if they could not get the investment back in the form of license fees or sales.

* **Various techniques which are mainly used for cyber crime.**

1. **Malware**

Malware is a general label for malicious software that spreads between computers and interferes with computer operations. Malware may be destructive, for example, deleting files or causing system ‘crashes’, but may also be used to steal personal data. There are a number of forms of malware.

* Viruses are one of the most well-known types of malware. They can cause mild computer dysfunction, but can also have more severe effects in terms of damaging or deleting hardware, software or files. They are self-replicating programs, which spread within and between computers. They require a host (such as a file, disk or spreadsheet) in a computer to act as a ‘carrier’, but they cannot infect a computer without human action to run or open the infected file.
* Worms are also self-replicating programs, but they can spread autonomously, within and between computers, without requiring a host or any human action. The impact of worms can therefore be more severe than viruses, causing destruction across whole networks (Beal, 2011). Worms can also be used to drop trojans onto the network system.
* Trojans are a form of malware that appear to be legitimate programs, but facilitate illegal access to a computer. They can perform functions, such as stealing data, without the user’s knowledge and may trick users by undertaking a routine task while actually undertaking hidden, unauthorized actions.

1. **Hacking**

Hacking is a form of trespass. It is the unauthorized use of, or access into, computers or network resources, which exploits identified security vulnerabilities in networks. Hacking can be used to:

* gather personal data or information of use to criminals;
* deface websites; or
* be employed as part of denial of service (DoS) or DDoS attacks (see below).

1. **Denial of service or distributed denial of service attack**

DoS and DDoS relate to the flooding of internet servers with so many requests (for example, links that have been clicked) that they are unable to respond quickly enough. This can overload servers causing them to freeze or crash.

1. **Spam**

Spam is unsolicited or ‘junk’ email, typically sent in bulk to countless recipients around the world and is often related to pharmaceutical products or pornography. Spam email is also used to send phishing emails or malware and can help to maximize potential returns for criminals.

* **How to be safe from cyber crime?**

In most cases, the implementation of these security measures takes only a few minutes. But these are very effective for protect us from cyber attacks. So, we have to aware about this.

1. **Install OS/software updates**. Updates, sometimes called patches, fix problems with an operating system (OS) (e.g., Windows XP, Windows Vista, Mac OS X) and software programs (e.g., Microsoft Office applications). Most new operating systems are set to download updates by default. After updates are downloaded, users are asked to install them. Click yes!
2. **Run anti-virus software**. To avoid computer problems caused by viruses, install and run an anti-virus program like Vipre, a product from Threat Track. Periodically, check to see if the anti-virus is up to date by opening the anti-virus program and checking the date of the last update.
3. **Prevent identity theft.** Never give out financial account numbers, Social Security numbers, driver’s license numbers or other personal identity information unless the recipient is known. Never send personal or confidential information via email or instant messages, as these can be easily intercepted. Beware of phishing scams – a form of fraud that uses email messages that appear to be from a reputable business (often a financial institution) in an attempt to gain personal or account information.
4. **Turn on personal firewalls.** Check computer security settings for built-in personal firewalls – and turn them on. Firewalls act as protective barriers between computers and the internet. Hackers search the Internet by sending out pings (calls) to random computers and wait for responses. Firewalls prevent computers from responding.
5. **Avoid spyware/adware.** Spyware and adware take up memory, and can slow down computers and cause other problems. Use Spybot and Ad-Aware to remove spyware/adware. Both of these programs are available online for free.
6. **Protect passwords.** Never share passwords. Establish a company “safe word” that a support technician requesting your work system login must know. Do not use one of these common passwords or any variation of them: qwerty1, abc123, letmein, password1, iloveyou1, (yourname)1, baseball1. Change your password periodically. When choosing a password, mix upper and lower case letters and use a minimum of eight characters.
7. **Back up important files.** Reduce the risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies. Store back-up media in a secure place away from your computer, in case of fire or theft. Test your back up media periodically to make sure the files are accessible and readable.

* **Some notable examples of ethics codes for IT professionals are listed below:**

### RFC 1087

In January 1989, the Internet Architecture Board (IAB) in RFC 1087 defines an activity as unethical and unacceptable if it:

1. Seeks to gain unauthorized access to the resources of the Internet.
2. Disrupts the intended use of the Internet.
3. Wastes resources (people, capacity, and computer) through such actions.
4. Destroys the integrity of computer-based information, or
5. Compromises the privacy of users.

### The Code of Fair Information Practices

The Code of Fair Information Practices is based on five principles outlining the requirements for records keeping systems. This requirement was implemented in 1973 by the U.S. Department of Health, Education and Welfare.

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

### Ten Commandments of Computer Ethics

The ethical values as defined in 1992 by the Computer Ethics Institute; a nonprofit organization whose mission is to advance technology by ethical means, lists these rules as a guide to computer ethics:

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

**Assignment Outcomes:**

Is there a difference between ethics in the real world and ethics online? While the answer to this question might seem obvious to parents, for many children, there is a very real and potentially dangerous disconnect between ethics in the real world and cyberspace. A recent poll found that nearly half of the elementary and middle school students who responded said they don’t believe hacking is a crime. Why is there this divide between real-world and cyber ethics, and what can parents do to make sure that their children practice ethical behavior when online?

Is the Internet that much different than the real world? After all, a crime is a crime. There are two characteristics of the Internet that make it difficult for children to transfer ethical behavior to the online environment:

The first characteristic is the feeling of anonymity. The *New Yorker* once published a cartoon with the punch line, “On the Internet, nobody knows you’re a dog”; the cartoon was making the point that it is easy to feel invisible on the Internet. Children often believe that they are “invisible” online because they cannot be identified and can get away with more (this actually isn’t true—modern computer forensics makes it very easy to track a user online). Many young children also feel that regular rules don’t apply to the Internet.

The second characteristic is distance. On the Internet, many people do and say things to others that they would never consider doing to someone face-to-face. Because children cannot see the direct consequences of their actions, they often think that what they are doing won’t harm anyone else. Of course, parents know that this is not true. Actions on the Internet still have the same repercussions as actions in the real world.

**Conclusion:**

In today’s world, the reality is that all individuals and organizations connected to the internet are vulnerable to cyber attack. The number, type and sophistication of attacks continue to grow, as the threat report published last month by the Australian Cyber Security Centre (ACSC) points out. It isn’t only large organizations that are under threat. Even individuals or organizations that don’t believe they have much to offer hackers can be targeted. So even if you think you’re a small target, you might still be at risk.

We can only get better at the defense part if we learn from previous experience, painful and costly as that may be. The reason we know about some of the attacks mentioned above is because they were detected and investigated. Children need to know that using the Internet is a privilege, not a right, and that improper use has consequences. Sitting down with your child and discussing these issues is the best way to make sure he does not use the Internet in a harmful or malicious way.

**References**

1. <https://en.wikipedia.org/wiki/Cyberethics> (last accessed: 30 August, 2018)
2. <https://en.wikipedia.org/wiki/Computer_ethics> (last accessed: 30 August, 2018)
3. <https://www.cerias.purdue.edu/assets/pdf/k-12/infosec_newsletters/07cyberethics.pdf> (last accessed: 31 August, 2018)
4. <https://www.ibsre.com/news/byline/cybercrime-the-importance-of-knowledge-preparation-vigilance/> (last accessed: 31 August, 2018)
5. McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*.
6. Namayandeh, M., & Taherdoost, H. Review Paper on Computer Ethics and Related Research Models.