

# Computer Ethics: What to practice and how?

**Authors: Anjusree Krishnanunni; Rachitha Dassanayake**

Nest Academy of Management Education, UAE

E-mail: [anjusree.k@nationalacademy.edu.in](mailto:anjusree.k@nationalacademy.edu.in),  
[rachitha.dassanayake@nationalacademy.edu.in](mailto:rachitha.dassanayake@nationalacademy.edu.in)

**DOI: 10.26821/IJSHRE.11.7.2023.110702**

## ABSTRACT

*The rapid growth of technology and other computing concepts have positive as well as negative impacts on the society. The misuse of computer technology by individuals and organizations have resulted for a need of new branch called "Computer Ethics". The term ethics normally refers to a set of moral principles and code that every individual has to follow. Computer Ethics is a field of ethics that consists of a set of procedures, practices and measures that has to be adopted by professionals working in computing technology and pertaining the moral and ethical values of the individual as well as the organization. It involves addressing the ethical issues while using the technology and methods that can be adopted to prevent or minimize the threats faced while working as computing professionals. Computer Ethics and Cyber Crime are like two sides of a coin because wherever there is a violation of Computer Ethics, there occurs a cybercrime. Basically, cybercrime are activities that targets a computer or uses a computer or a network with the intention of damaging or disabling the device/network. This can be done by criminals popularly known as cyber criminals or by the irresponsible actions of individuals. The main aim of cybercrime is financial although in some cases it might be for other personal gains like to take revenge or personal satisfaction. As technology is growing day by day and the activities and transactions are dependent on internet, organizations and individuals fail to comply with the code of Computer Ethics which makes it even harder for people to stay away from cybercrime and become a victim of it. With an increase in the number of cybercrime cases, there is a huge loss of social value as well as property damage to the public. Thus, we have to ensure that there are strict rules and security features in place which can ensure people for safe usage of computers is a secure environment. The users have to be aware of the diverse forms of cybercrimes that are occurring around them and the magnitude of the danger it can cause. This awareness has to be created among children, teenagers, adults as well as the government so that the public will be take all necessary precautions to stay safe.*

**Keywords:** *Cybercrime, Hacking, Spamming, Phishing*

## 1. INTRODUCTION

The rapid growth of technology and other computing concepts have positive as well as negative impacts on the society. The misuse of computer technology by individuals and organizations have resulted for a need of new branch called "Computer Ethics". The term ethics normally refers to a set of moral principles and code that every individual has to follow. Computer Ethics is a field of ethics that consists of a set of procedures, practices and measures that has to be adopted by professionals working in computing technology and pertaining the moral and ethical values of the individual as well as the organization. It involves addressing the ethical issues while using the technology and methods that can be adopted to prevent or minimize the threats faced while working as computing professionals.

The primary focus of Computer Ethics is the ethical use of all the computing resources. This comprises of all the practices and procedures that will avoid violating copyrights and the unauthorized selling and buying of digital content. The major issue bound with computer ethics is from the usage of internet because of violation of Internet privacy. The users are exposed to different threats and attacks while using internet.

Computer Ethics and Cyber Crime are like two sides of a coin because wherever there is a violation of Computer Ethics, there occurs a cybercrime. Basically, cybercrime are activities that targets a computer or uses a computer or a network with the intention of damaging or disabling the device/network. This can be done by criminals popularly known as cyber criminals or by the irresponsible actions of individuals. The main aim of cybercrime is financial although in some cases it might be for other personal gains like to take revenge or personal satisfaction.

As technology is growing day by day and the activities and transactions are dependent on internet, organizations and individuals fail to comply with the code of Computer Ethics which makes it even harder for people to stay away from cybercrime and become a victim of it.

## **2. RESEARCH METHODOLOGY**

The paper aims to analyze the concept of Computer Ethics, the dependence of computer ethics with cybercrimes, the popular cybercrimes and some methods that can be used to stay protected and safeguard the users from cybercrimes. Intensive secondary research has been carried out to understand the impact of Computer ethics in different areas of technology and the changes and effects of using them. Secondary data was collected from journals, books, magazines, and research monographs.

## **3. COMPUTER ETHICS: A DETAILED ANALYSIS**

Ethics generally deals with social attributes, human behavior, and other policies. Ethics always helps us to distinguish between good and bad, what is the right thing to do and what is not to be done. Computer Ethics basically is a set of principles that regulates and manages the use of computers. Some of the main issues of computer ethics includes intellectual property rights that comprises of copyrighted content, privacy matters and concerns and various effects of computers on society. Computers and technology provide us with new capabilities and opens doors for new choices of actions. Computer Ethics have evolved tremendously for the past few years due to its importance as well as due to the fast growth of technology. A central task of Computer Ethics is to analyze different scenarios of violation, breach of security and privacy and to determine the actions that has to be done to overcome them and the steps that can be adopted to make sure that it will not reoccur. The existence of computer ethics is required for the social well-being of people, to promote privacy respect, safety of the users and creation of job opportunities.

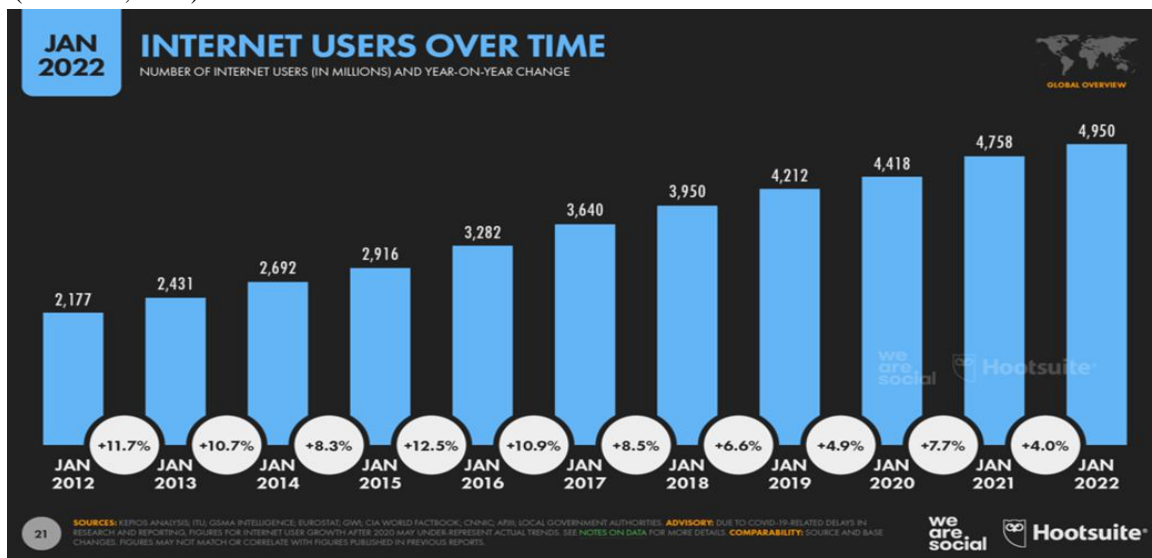
Computer Ethics have many positive impacts on individuals, organizations, and the society. They help to foster computer knowledge and leads to a better understanding. It generally helps to create an awareness of the good and bad outcomes of using computers and staying online. As we all know computers store a variety of data. It helps to enhance the safety of data. A good understanding of computer ethics promotes honesty, trustworthiness, and increases societal well-being. They make sure that property rights are maintained, followed, and honored. They help to reduce or eliminate the spread of false information and also avoids the misuse of personal information. Computer Ethics plays a very crucial role for all internet applications to prevent frauds. As the internet and cyberspace are shared mutually with everyone all over the world, all the countries must collaborate, on an international level, to defend against this broad range of threats.

### **The 10 Commandments of Computer Ethics**

The concept of 10 commandments was put forth by the Institute of Computer Ethics in the year 1992. It is a set of general principles we have to follow while using computers.

- 1: Do not use the computer to harm other people's data.
- 2: Do not use a computer to cause interference in other people's work.
- 3: Do not spy on another person's personal data.
- 4: Do not use technology to steal personal information.
- 5: Do not spread misinformation using computer technology.
- 6: Do not use the software unless you pay for this software.
- 7: Do not use someone else's computer resources unless he authorized to use them.
- 8: It is wrong to claim ownership of a work that is the output of someone else's intellect.
- 9: Before developing software, think about the social impact it can of that software.
- 10: While computers for communication, always respectful with fellow members.

(Ramon C, 1992)



**Figure 1: Graph representing the increase in the number of internet users all over the world (Simon,2022)**

The above commandments are put into practice since many years now, but the real question is are everyone practicing them. Computers have becoming very powerful, and the IT professionals are like wizards controlling this technology.

#### 4. COMPUTER ETHICS AND CYBERCRIMES

Ethical Issues are problems or issues that requires people and organizations to decide between the choice of evaluation – What is evaluated as right (ethical) and what is evaluated as wrong (unethical). Whenever the ethics are broken by individuals or organizations, cybercrime occurs. Cybercrimes are intellectual, white-collar crimes. The hackers/attackers who commit such crimes generally manipulate and modify the systems in a very intellectual and technical manner.

##### 4.1. Common Unethical Computing Practices

The internet is an insecure channel for exchanging data and information. The main reason for it is that while we are on the internet, we are exposed to various types of threats and fraudulent activities. There are different types of unethical practices that can cause partial or full breakdown of devices and networks. So, it is important to create an awareness among the users about such malicious activities and attacks that is common nowadays.

1. Cyberbullying

It is the practice of bullying other people by the use of electronic devices and communication channels like internet, social media and so on. This could be done by friends, relatives, or any other unknown persons as well. Some coming ways of cyberbullying includes sending harmful emails, creating fake websites to cheat people, following on social media, and passing hurtful/cruel comments, stealing online identity and so on. The bullied persons are affected in many ways like emotional or mental breakdown, depression, financial loss and so on.

How to overcome Cyberbullying: It is always best not to respond to cyberbullying. Don't open the emails you receive from unknown sources and senders. Also never reveal your passwords to anyone. Be careful when posting photos and videos online.

## 2. Phishing

This is also a type of internet hacking activity. In this, the hackers send email to the users under the pretext that it is from trusted organization so as to mislead the users. The attackers generally ask the users to visit the mentioned website and once they open the website, they will be asking for the users' personal information including passwords, credit card information or other personal details and use that information for illegal and unethical purposes.

How to overcome Phishing: Do not open any documents or links or images sent from unknown people. Do not share any personal information through phone or email with some known person. Make sure you have an active and updated firewall on your computer. Check the bank statements on a regular basis to make sure that no unauthorized transactions are made without your consent.

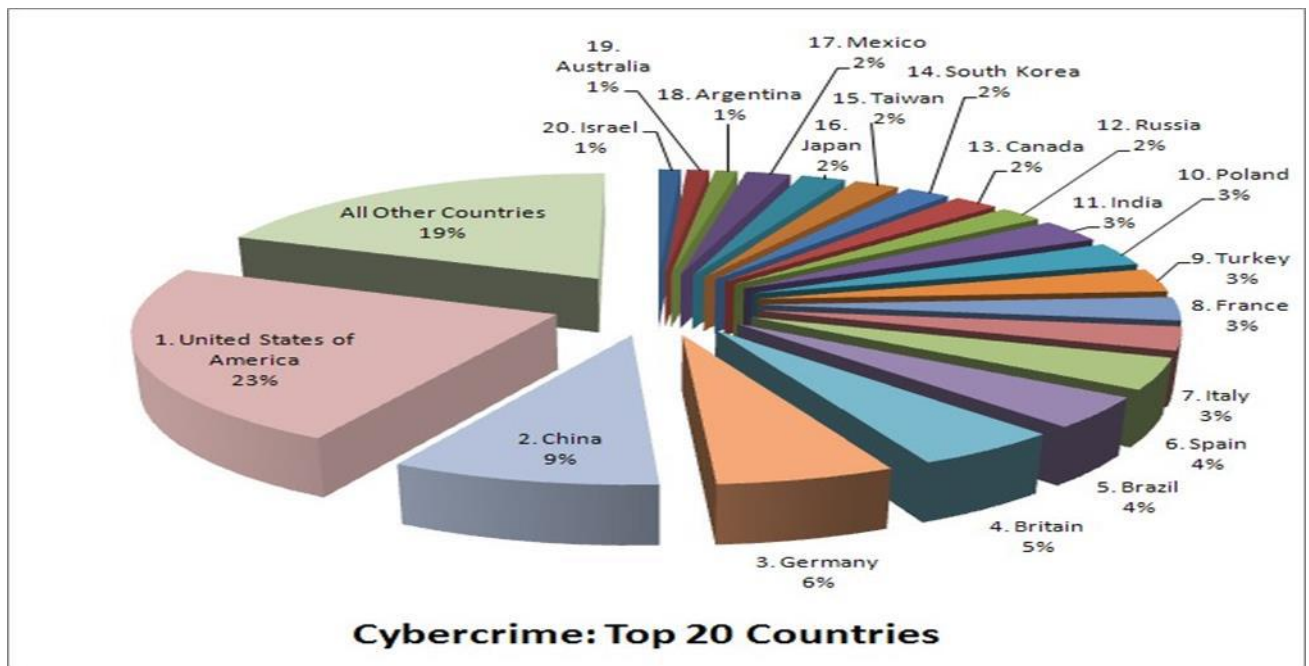


Figure 2: The percentage of cybercrime in Top 20 countries (EngimaSoft, 2021)

## 3. Hacking

It is the unethical activity where in skilled professionals called hackers enter into the computer of another person without his/her permission and then steals the important things from the computer which can be data, applications or the entire project. Sometimes the hackers end up destroying the data as well.

How to overcome Hacking: Do not connect your devices and systems to a free Wi-Fi or a public network. Make sure to use strong passwords (at least 8-bit long password which is a combination of uppercase, lowercase, numbers, and special characters). Keep your operating system updated. Make sure you have softwares like Anti-virus and Anti Malware softwares.

#### 4. Spamming

In this type, bulk unwanted emails are sent from strangers or any unknown sources. In most of such cases, due to these emails, the email serve becomes full and then mail bombing happens. Spam emails are generally used to deliver many types of attacks which can be worms, trojan horses, viruses, spyware, malware etc. which will attack the users.

How to overcome Spamming: Install some filtering software that would check all the incoming emails and block the spam emails.

If you find any suspicious email in the inbox, then immediately delete such emails. Always keep the all the software updated. Also do not open links sent from unknown people.

#### 5. Viruses

They are commonly attached to downloadable files like word documents, images or are automatically downloaded into your system when you open certain websites. Once we open such corrupted files, the virus will start to exploit all the vulnerabilities that the system has and will attack the system. The system under attack can lose data, disrupt network traffic,

How to overcome Viruses: Always install antivirus softwares in your computers. Never open websites that you don't have "https" in the URL. Do not download attachments from unknown sources. Always scan your system for viruses and make sure all the softwares are updated.

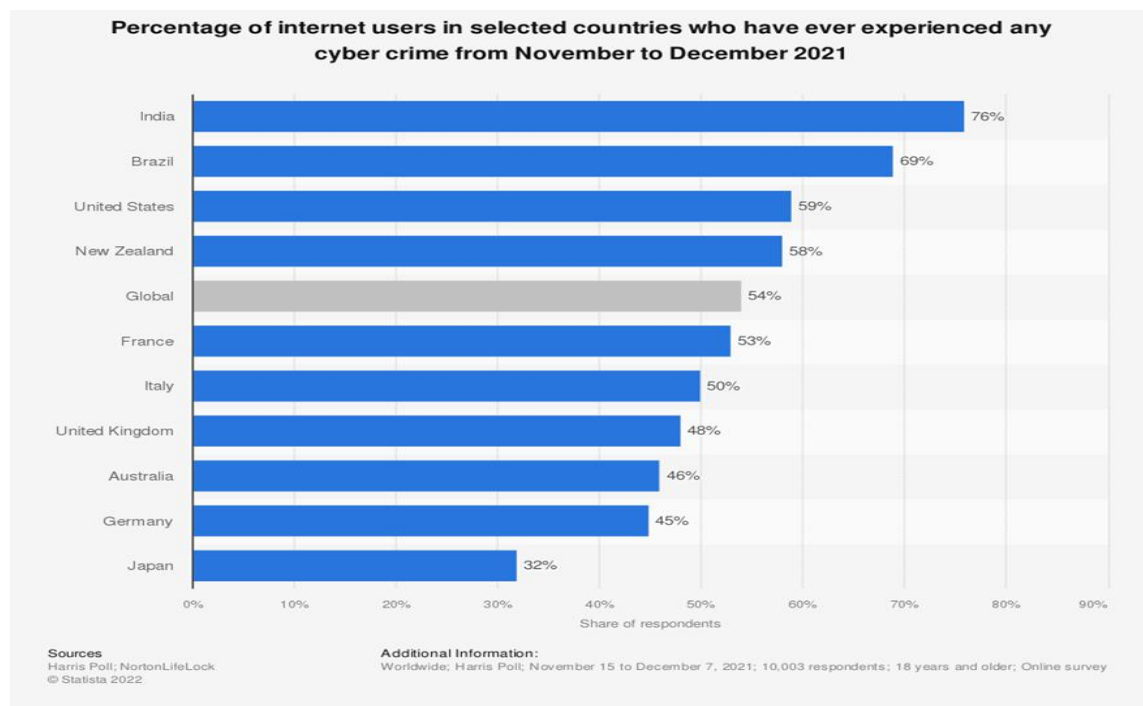


Figure 3: Graphical Representation of the users facing cyber-attacks as per country (Statista, 2021)

## 5. ACKNOWLEDGEMENT

We would like to extend our wholehearted thanks to all our colleagues and friends who helped us and guided to complete this paper. Special thanks to our institution for all the support.

## 6. CONCLUSION

Computer Ethics has to be followed and practiced by our own free will and not something that is to be forced on us. Because of the lack of effective supervision and proper legislation, there can be ethical and moral problems occurring frequently while using computers. There is a tremendous increase in the number of online users and a growing dependence on technology which has made it difficult for everyone to follow the moral requirements. With an increase in the number of cybercrime cases, there is a huge loss of social value as well as property damage to the public.

Thus, we have to ensure that there are strict rules and security features in place which can ensure people for safe usage of computers is a secure environment. The users have to be aware of the diverse forms of cybercrimes that are occurring around them and the magnitude of the danger it can cause. This awareness has to be created among children, teenagers, adults as well as the government so that the public will be take all necessary precautions to stay safe.

## 7. REFERENCES

1. Sarkari Update | Education || Job Update. (2022). *Sarkari Yojana 2022 List, News, Updates / PM Modi Yojana 202*.
2. Bartleby.com. (2020). *Computer Ethics Essay / Bartleby*.
3. ResearchGate. (n.d.). (PDF) *Cyber Crime & its Categories*.
4. Vallor, S., William, J. and Rewak, S. (n.d.). *An Introduction to Cybersecurity Ethics*.
5. GeeksforGeeks (2021). *Computer Ethics*. [online] GeeksforGeeks..
6. Kemp, S. (2022). *Digital 2022: Global overview report*.
7. *The Handbook of Information and Computer Ethics*. (2008).
8. Sareen, M. (2020). Computer Ethics and its related issues. [online] 8(9), pp.2320–2882.
9. *Cyber Crime: Its Impact on Government, Society and the Prosecutor An Aid for Assisting the Prosecutor in the Investigation, Trial and Conviction of the Cyber/Computer Criminal*
10. Gunarto, H. (n.d.). *Ethical Issues in Cyberspace and IT Society*.