Cyber Ethics in Security Application in the Modern Era of Internet

Megha Sharma*
Sanchit Mittal**
Ankit Verma***

Abstract

Societies are becoming more dependent on computer networks and therefore more vulnerable to cyber-crime and internet terrorism. In this paper we have discussed the different ethics of cyber world. In layman terms ethics are the "code of conduct" or the protocols which every responsible citizen should follow while using an internet facility. Here we are mainly concerned with the reasons behind inventing the internet network, and understanding the positive and negative usage of internet, and analyzing the behavior of internet users, and how it affects individual's life and Indian societies in this modern technical era. Computers raise various problems such as privacy, ownership, theft, illegal use and power. So the main purpose of this article is to provide a glimpse of cyber world including the cyber ethics, cyber-crime and preventive measures to deal with these cyber-crimes.

Keywords: Cyber Crime, Cyber Ethics, Cyber Security.

Introduction

In the society where we live, everyone has to accept some kind of rules, values, culture and has to deal with the thinking of people i.e. we need to follow some code of conduct to survive in that particular place. In the same way the ethics in cyber world may referred as the branch of philosophy which deals with values of human behavior, with respect to the rightness and wrongness of certain actions and to the goodness and badness of the motives and ends of such actions. In simple terms Cyber ethics is the philosophical study of a system of moral principles pertaining to computers [1]. In today's era the internet is growing vastly in terms of its users. Everyone is addicted to the usage of internet, as most Internet users are convinced with its general utility and positive benefits. The internet is the medium of connecting people through a large worldwide network. Internet has proven tremendously useful in this modern world of technology However, in consequence of the growing internet usage it is leading to some bad or illegal activities such as: cyber stalking, hacking, phishing, cross-site scripting, cyber extortion, fraud and financial crimes. Therefore Measures to protect information systems have received increasing attention as the threat of attacks grows and the nature of that threat is better understood. Among these measures are sophisticated technologies for monitoring computer networks and users, detecting intrusion, identifying and tracing intruders, and preserving and analyzing evidence.

Megha Sharma*
Student (BCA) IT
IINTM, Janakpuri, New Delhi

Sanchit Mittal**
Student (BCA) IT
IINTM, Janakpuri, New Delhi

Ankit Verma***
Assistant Professor IT
IINTM, Janakpuri, New Delhi

Internet - A Blessing or A Curse

Internet is a vast computer network linking between computer networks globally. The internet involves educational, governmental, commercial and other networks, all of which use the same communication cycle. The world of Internet today has become a parallel to life and livings. Humans are now able of doing things which were not imaginable few generations ago [2]. The Internet has become a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on the

machines. Internet has enabled the use of website communication, email, surfing and a lot of anytime anywhere IT solutions for the betterment of human beings. Though, internet offers great advantages to society. It also presents opportunities for crime using new and highly sophisticated technology tools. Regular stories featured in the media on computer crime include topics covering hacking to viruses, web-hackers, to internet paedophiles, sometimes accurately displaying events, sometimes misconceives the role of technology in such activities. Increase in cyber-crime rate has been shown in the news media. The increase in the incidence of criminal activity poses challenges for legal systems, as well as for law enforcement to take active and fast decisions. The internet network has definitely proved a great blessing to the human kind. It should be our responsibility to utilize technology in a positive way to compete with this rapid world. Every coin has two faces. It's up to us to receive well and to leave bad [3].

Cyber Ethics

Cyber ethics is the study of moral, legal, and social issues including cyber technology. It explores the impact that cyber technology has for our social, legal, and moral systems. It also ascertains the social policies and laws that have been framed in response to issues generated by the development and use of cyber technology. Hence, there is a common relationship [4]. Cyber ethics is a dynamic and complex field of study which considers the interrelationships among facts, observations, experiments, policies and values with regard to constantly changing computer technology. Data processing today is much faster, more flexible, and better arranged and portrayed than ever before in our history. Every technology has introduced not only new opportunity but also new risk. A responsible citizen must follow these cyber ethics to avoid adverse result.

Cyber Crime

Cyber-crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a technique, or a field of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to comprise traditional crimes in which computers or networks are used to enable the illicit activity [3]. Internet is certainly the forest of the information and because of its lack of control and restrictions, the Internet aid as a potential threat to society. The various crimes associated with computers are difficult to evaluate in terms of either size or frequency, but it sound safe to say that the number and variety are increasing and the stakes are growing.

Cyber Crime Variants

There are a large number of cyber-crime variants. A few varieties are discussed for creating the awareness. This article is not intended to expose all the variants hence we have enlightened some of the major issues subjected to the risk in cyber world.

Hacking. "Hacking" is a crime. It is the way of gaining unauthorized access to a computer and viewing, copying, or creating data without the intention of destroying data or maliciously harming the computer. In broad terms we can say that hacking is used to describe many complex activities wherein the end goal is typically to obtain access to server, databases or stored files of a computer system [4]. This access may be any combination or desired or undesired, and lawful or illicit.

Phishing. Phishing is the attempt to acquire sensitive information such as login id , passwords, credit card information and other personal detail to access someone's account for some reason by masquerading as a trustworthy entity in an electronic communication. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they abide unsuspected that the fraud has occurred [3]. The swindler then has access to the customer's online bank account and to the funds contained in that account.

Cyber Stalking. Cyber stalking is the use of the Internet or other electronic means to stalk or harass users. It may include wrong accusations, defamation, slander and libel. It also involves monitoring, identity theft, threats, vandalism, or gathering data that can be used to threaten or harass. Stalking generally involves harassing or threatening behavior that an individual engages in continuously, for example following a

person, appearing at an individual's home or in business organization, making harassing phone calls, or vandalizing a person's property. There are a wide variety of means by which individuals may seek out and harass individuals even though they may not share the same geographic borders, and somewhere it presents a variety of physical, emotional, and psychological results to the victim.

Cross-site Scripting. Cross-site scripting, or XSS, is a method of injecting harmful code and links into another safe website's code. It is one of the most commonly used techniques of hacking. As Web browsers have built-in security to prevent a range of XSS attacks, hackers can still exploit flaws or imperfection in the program to convince the browser that planted code is trusted. Examples of such code include client-side scripts and HTML code. The attackers can use an exploited cross-site scripting vulnerability to bypass access controls [5].

Cyber Extortion. Cyber extortion is a crime involving an attack or threat of attack against a venture, coupled with a demand for money to stop the attack. Cyber extortion can be of many forms. Originally, denial of service attacks was the most common method. As the number of enterprises that rely on the Internet for their business has expanded, therefore opportunities for cyber extortionists have exploded.

Cyber Security – Protect Yourself

The Internet operates and functions largely on a collaborative basis. Its smooth functioning depends heavily on the proper conduct of users. In this technological era our protection is only in our hands, we should act as an aware and responsible user of this technology [5]. Below we list a set of good practices that make the Internet a better place for all users.

Using webmail wisely

- Usually the default setting of social networking website is to allow anyone to see your profile. You can change your settings to restrict access to only authorized people.
- Select only trusted and well-known webmail service providers.
- If you use a public computer to check your email. Read the tips that what security points should one kept in my mind while using a public computer, If an individual access his/her webmail account using a shared computer, remember to remove the data in cache memory, cookies, and other temporary buffer space that might hold your email attachments before you leave the machine.

Be a Responsible Internet User

As a responsible Internet user, you should protect your system and data with adequate security techniques [4]. An Individual must maintain a Good habit in handling of emails, password management, usage of software, web surfing and downloading files, will help in securing your computer from attack.

Be a Law-abiding Internet User

- Do not perform any activity which is illicit, fraudulent or prohibited under any applicable legislation.
- Do not publish post, distribute, or disseminate libelous, infringing, obscene, or other illegal material.
- Do not transmit, download or upload data, information, or software in violation of any applicable legislation. It involves, but is not limited to, data protected by privacy and copyright laws.

Self-Awareness for Information Security

- One should take it as his/her responsibility in keeping own information secure from external misuse.
- An individual should keep equipped with the latest knowledge and must be alert to the news regarding security threats.
- If any person is in doubt, then they must consult advisers or experts.

Handling user accounts carefully

- Use a password of at least six mixed-case alphabetic characters, numerals and special characters.
- Change your password frequently
- Change your password immediately if you believe that it has been steal by some other person. Once done with making change in the password, notify the system or security administrator for follow up action.

- Always do remember to Log out from your account when finished using public pc, such as in a library.

Handling your personal information

- Make your account and password secure with the available security mechanisms.
- Encrypt/secure the sensitive data when transferring personal information over public networks such as the Internet.
- Always be wary when giving out sensitive personal or account information over the Internet. Banks and financial institutions rarely ask for your personal or account information via email or over the web.

Be a Good Neighbor in Internet Community

- Do not perform any activities which may interfere with other users or restrict or hinder any person from accessing, using or enjoying the benefits of Internet.
- Do not access, use or monitor any data, networks or system, including an individual's private information, without any authority or his/her permission.
- Do not attempt to conduct any network/port scanning or hacking activities on other computers.
- Do not send or distribute links or source of any computer virus, malicious codes or harmful programs.

Conclusion

Internet has been invented for the betterment of humans. Internet has its own boon and bane. However it's our choice to use this invention for betterment of society or to produce harm to others. The ill activities taking place through internet are grouped under cyber-crimes and are also taken care by some cyber authorities by stating some policies, protocols, preventive measures etc. An individual must be aware of cyber ethics i.e, the protocols followed while using an internet network; cyber-crimes, crimes taking place in the cyber world and what are the risks while working on internet; and what are the possible ways to protect ourselves from being attacked by these cyber criminals. Strict penalties must be taken by the law if someone tries to mishandle the use of internet and to harm others for own benefits over internet. Cyber authorities should also aware the people about the threats and what protective measures could be taken. Government should also take remarkable steps towards the criminals indulging in such offences. At a point our protection is in our hands first so must follow the preventive measures and take care of some points discussed in this article to protect yourself from cyber-crimes.

References

1. ACM, 1992, ACM Code of Ethics and Professional Conduct, Association of Computing Machinery, USA, October 1992.
2. Chan, Serena and L. Jean Camp, 2002, Law Enforcement Surveillance in the Network Society.
3. Berinato, Scott; "Debunking the Threat to Water Utilities", CIO Magazine, CXO Media Inc., March 15, 2002.
4. Stephanou, Tony; "Assessing and Exploiting the Internal Security of an Organization", The SANS Institute, March 13, 2001.
5. FX, "Attacking Networked Embedded Systems" CanSecWest Conference, Vancouver, May 2003.