IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber - Crime And Its Prevention: A Study

Dr. Sukumar Das
Assistant Professor
Department of Philosophy
Sibsagar University
Sivasagar, Assam

Abstract: The history of technology is as old as the history of global society. The invention of the computer is an electronic device of new technology. The computers are a necessary and essential part of human life far and wide. In this new invention of technology, all possible crime committed in the computer is generally known as cyber-crime. The cyber-crime is computer-centric crime. This crime is associated with computer network. This crime is one of the most complex and critical problem in the digital age which is affecting individuals, organizations and government work. With the rapid growth of science, technology and internet aperture, criminal activities like hacking, phishing, ransom ware, cyber stalking, and financial frauds have desperately increased. This research paper aims to analyze the nature, forms and causes of cyber-crime and also to highlight the preventive measures, and technological of safeguards designed to take up against cyber-crime and to raise awareness in today's world. It also highlights that through awareness we can protect all their personal data in the online world.

Index Terms - Technology, Computer, Cyber, Crime, Hacking, Phishing

Discussion:

We see various crimes like robbery, kidnapping, rape etc. all around us. A similar type of crime is computer-centric. The current era is computer era. Like the crime prevalent in our society, various crimes are committed in the computer world every day. Computer-centric crimes are commonly referred to as 'computer crimes.' It is also called 'cyber-crimes.' Cyber-crime is any illegal activity which is implicated the use of computers, electronic devices, or the internet. It refers to illegal acts carried out in cyberspace where technology is the tool, the target, or both. There is no statutory definition of cyber-crime in Indian Laws under the IT Act. It can be defined as: "Any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime."[1]Cyber-crime is broadly defined as unlawful acts committed using computers, networks, or digital

[1] Definition by Royal Canadian Mounted Police in 2000, as quoted in Sameer Hinduja: Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future, International Journal of Cyber Criminology, Vol. 1 Issue 1, January, 2007

devices. It is a crime of computer or computer network. Cyber-crime is the direct or indirect use of computer hardware, software, networks, resources, data or information to commit any illegal act. With the computer revolution, cyber-crime has increased in the world. Cyber-crimes usually occur over various networks, the internet and memory devices. This crime affects personal business practices, personal security and even personal computers.

Debarati Halder and K.S.K Jaishankar defines cyber-crime as "intentional or direct defamation against an individual or group of individuals with criminal intent using modern telecommunication network, such as the internet (chat com, email, notice board and groups) and mobile phones (SMS and MMS). Cyber-crime is indirectly causing physical and psychological harm, or harm" (D. Hader & K Jaishankar: Cyber-crime and the Victimization of Women: Laws, Rights and Regulations). Cyber or computer crime poses a threat to the security and financial security of a nation. A violation of privacy occurs when certain information is intercepted or disclosed legally or illegally. Crimes like hacking, copyright infringement, child pornography are now hugged. They have taken on the form. Using the modern networking techniques of the internet and mobile phones, many people have deliberately tried to harm women physically and mentally. Cyber-crime has taken an extreme form in various fields such as financial fraud, national or international data theft. In addition, in the world today, Acro basters are engaged in cyber warfare against tradition in various ways, directly or indirectly, by capturing confidential information of one country, causing financial damage, harassing the people of other countries, etc.

It is not possible to say exactly what cyber-crimes are. One thing can be clearly stated, if an immoral act is committed against someone in private and public life through computer-centric activities without his knowledge, it will be considered as a cyber-crime. "The Association of Information Technology Professionals (AITP) has defined the following as computer crimes.[2]

1. The unauthorized use, access, modification and destruction of hardware, software, data or network resources by unauthorized persons.
2. The unauthorized release of information.
3. The unauthorized copying of software.
4. Denying and end user access to his or her own hardware, software, data or network resources.
5. Illegal access to any information or specific resources using or conspiring to use computer

Objectives of the Study:

1. To define and classify the nature and scope of cyber-crime.
2. To analyse the types of cyber-crime.
3. To analyse the root causes, motives and contributing factors leading to the rise of cyber-crime.
4. To suggest practical recommendations and prevention strategies for minimizing cyber-crime.

[2] "Factors Affecting Computer Crime Protection Behavior" page 3 by Sirirat Srisawang, Mathupayas Thongmak, Atcharawan Ngarmyarn

Methodology:

1. Research Design:

The study of the research paper is an analytical and descriptive research. It is not only qualitative but also quantitative approaches. It focuses on forms, causes, influence and preventive measures of cyber-crime through secondary data analysis.

2. Secondary Data Sources:

Books, peer-reviewed journals, cyber security agency publications, legal documents, and case studies related to cyber-crime.

Different forms of Cyber-Crime:

Cyber-crime is many forms. Some forms are as below:

1. Child Pornography: Production of child pornography made or distributed. It includes criminal acts such as displaying selling or selling nude or semi-nude images, videos, content etc. of a child through computers or the internet.
2. Copyright Violation: Using another's work without permission, Stealing or using a person's copyrighted material. This type of crime includes claiming and using information from Google or Wikipedia and the internet.
3. Cracking: Cracking is a computer or the internet stealing, destroying and illegally accessing any information, data by entering. This breaks the codes progress for data protection.
4. Cyber Terrorism: Cyber terrorism is internet-based terrorist activities. Such crimes include hacking, intimidation or blackmailing a business or individual.
5. Cyber Stalking: Any group or organization using the Internet or another electronic device shall be subject to disciplinary action, falsely accusing slander, publishing defamatory articles etc. are cyber stalking.
6. Cyber Squatting: Cybersquatting is unauthorized involved in pollination and internet domain management. Cybersquatting is the setting up of a domain of a blessed person or organization for the sole purpose of selling it at a premium price, using similar trademarks, service marks, company names or personal names.
7. Malware crime: Creating, making and distributing of malware such as viruses and spyware are one types of cyber-crime.
8. Doxing: Doxing is form of cyber-crime. Doxing is personal information which disclose without the permission of concern person. Sharing anyone's personal pictures or videos without permission of the concern person is considered doxing.
9. Software Piracy: Software Piracy Software pirating is unauthorized copying, distribution, revision, selling, or use of fairly defended software, basically" stealing" it and violating brand laws and software licensing agreements

10. Spamming: Spamming is some information which is sending to different people at once. Sending the multitudinous unsolicited e-mails to various addresses is called spamming. It is used to send ads, repeated messages on the same site. E.g. Instant message, mobile phone message, internet forums, Junk, blogs wikis online classified advertisement, mobile apps etc. are called spamming.
11. Hacking: Hacking is the unauthorized gain of access to a computer system, network or data. The main purpose of hacking is to damage the system. the individual who are involved in such type of hacking is called hacker.
12. Vishing or Voice phishing: Voice phishing is one type of phishing through use to telephone or audio. Vishing or voice phishing is committed by making telephone calls or computer calls to inform a person that he has won the lottery or by offering money or by providing sensitive information on a fake website by offering bank account verification.
13. Spoofing: The literal meaning of spoofing is to disguise or impersonate something or someone else to deceive others, often to gain trust, steal information, or commit fraud. In the field of information technology, spoofing is the act of deceiving any computer user or computer system by employing tactics. That is, when cybercriminals conceal their identity or forge the identity of another user to gain access to a computer or take control of it under the guise of a trusted or depend on source, it is referred to as spoofing.
14. Stealing intelligence Assets (Stealing Resource): Stealing intelligence Assets is the stealing practical or conceptual information developed by another person or organization.
15. IPR Violation: Intellectual property rights infringement is an infringement of another's copyright, patent or trademark.

Prevention of Cyber-Crime:

Identification of cyber-crime and prevention or punishment is a great challenge in today's life. In many cases, it is impossible to arrest the perpetrators once they are identified. However, it is seen that the increase in technological skills and knowledge of the internet has made it easier to take various measures to prevent cyber-crime. The following measures can take to prevent or counter the offence of cyber crime

Investigation: Just as computers are a source of crime, they are also a significant source of evidence. When someone uses a computer directly for criminal activities, some information is stored on the internet which can be easily traced to identify the criminal by a skilled person. Even in cases where a computer is not directly used for criminal activities, there may still be criminal records in the form of log files. In most countries, internet service providers are required to retain their files for a predetermined period of time.

Making Laws: Due to the presence of various simple laws, cyber criminals do not feel any hesitation in committing such crimes. Even after committing a crime, they easily evade the law and continue to engage in similar criminal activities. In some countries, cyber-crime laws are merely nominal, such as in the Philippines, where cybercrime laws are just a formality.3 Many such laws exist only nominally in developing countries, making them a target for cyber-criminals. Due to weak laws, even if criminals are identified, they can be assured by citing international borders. Because of weak laws, a criminal is protected from being extradited

[3] https://en.wikipedia.org/wiki/Cybercrime

from one country to another. Therefore, to prevent cybercrime, there is a need to formulate strict and strong laws. By formulating strict laws, the fear of severe punishment will somewhat reduce cyber-crime.

Punishment: Often the punishment for criminals becomes so minimal or minor that they are encouraged to commit such crimes. There should be a proper system in place to ensure that criminals receive appropriate and exemplary punishment. Only then will the cyber-crime be prevented, as this crime is increasing day by day.

Awareness: Public awareness is one of the ways to prevent cyber-crime. The personal information, number, code number, OTP, password should never share or given to unknown persons in any way. Today's world is world of technology, every moment people used and based on internet and computer. Therefore, criminal are constantly increases and try to steal banking details and credit, debit card information. Cyber-criminal is trying to collect people's personal information by various inducements and tricks. Hence, should not share or give personal information and any others data to unknown persons, does not click any unknown link, phone call or any unknown application. Therefore, it is essential to create awareness among the mass people about the criminal's tricks and what tactics they have been used. There is a great need to raise awareness about this in today's world. Everyone should be aware of how to protect all their personal data in the online world. Prevention is better than cure.

Conclusion:

Today the Computers are a necessary and essential part of human life far and wide. It plays an important role in all areas of human activity, including education, business, healthcare, industry, government work, and information exchange. Social welfare efforts have been able to make a revolutionary contribution through computers. Therefore, computer experts have certain professional responsibilities and duties in social welfare. If they remain ethically honest, they can prevent cyber-crimes or misuse of computers through their work. They need to develop software or applications that are not harmful to people's lives, which can lead modern society to reach the highest levels of development in the near future.

Reference:

1. 12 Ways to Prevent Cyber Crime, Article by Siman Burge, International Security Journal, Published April 7, 2024
2. India: Cyber Security 2020, ICLJ.com February 22, 2019) https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india
3. Holmes, R.L. Introduction to Applied Ethics, Bloomsbury Publishing, 2018.
4. Cyber Law-Law of Information Technology and Internet, Rastogi Anirugh Assisted by Asheeta Regidi, Lexis Nexis4th Floor, Tower B, Building No. 10, DLF Cyber City, Phase-II, Gurgaon - 122002
5. Applied Ethics, Bora Dr. Manashi, A text book on Philosophy, Union Book Publication, Panbazar, Guwahati-1, Assam
6. Prayogik Nitividya, A text book of Philosophy, Roy Hemanta Kumar, Union Book Publication, Panbazar, Guwahati-1, Assam
7. https://en.wikipedia.org/wiki/Cybercrime