CYBER SECURITY: TYPES AND CONSTITUTIONAL PROVISIONS

Submitted by:

Dr. Sushma Rani

HOD & Associate Professsor

School of Education, Lingaya's Vidyapeeth, Faridabad

Abstract

Cyber crimes are similar to any crime, but it involves computers and networks. In some cases, computers can be used to commit crimes, and in other cases, computer crime may be the target. It includes everything from stealing millions of dollars from online bank accounts to downloading illegal music files. Cyber crime also involves transactions involving non-money transactions, such as spreading viruses on other computers or posting a private information of any business on the Internet. Cyber Criminals can use computer technology to access your personal information, to know the secret of the any trade or use the Internet for other malicious purposes. Criminals who do such illegal acts are often called hackers. This paper deals with the various types of Cyber-Crime and their influence on the society and masses.

Keywords: ***Cyber Crime, Cyber Security, Hacking, Phishing, Logic Bomb***

Introduction

There are hundreds of ways to cybercrime, in which cyber crime can be explained, and you have to know what they are.

Since, cybercrime is a crime that is done by the help of a computer and a network by a person using computer internet software etc. Using any of the techniques, causing any kind of harm to another person, company etc. is called cybercrime.

That is, the weapon to commit a crime is not a gun knife or a bomb, but this weapon is the computer internet through which people commit crimes under which it is to steal information from someone's computer, by deleting someone's information. Using such crime, these can be obtained in a variety of ways like sending spam emails and hacking by inserting viruses etc.

Types of Cyber Crime

Spam-Email: There are many types of emails coming in our email account, which also include emails which not only harm the computer but also wastes user's time. Spam is the kind of e-mail that comes without asking, in which the advertisements are usually filled, thus it proves to be a problem since email has evolved. A study from April 2008, revealed that atleast 100 billion spam is sent everyday, for sending

spam, the information to be sent to spam emails are collected from the chat rooms, websites or several viruses. The example of spam is sown as below in the fig. no.-1

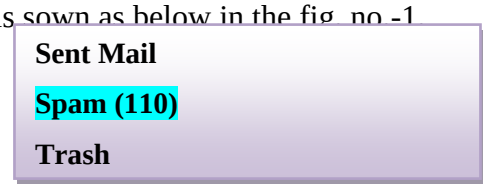

Fig. No.-1 (Spam E-mail)

Hacking: Hacking any personal information such as a user's name or password and then manipulating it is known as computer hacking. Hacking means unauthorized infiltration and manipulating data in network software a computer device information system. In simple words, hacking is a task in which a hackers access your computer or server without your permission. Hackers (people who 'hacking') are basically computer programmers who understand the computer's advance and generally abuse this knowledge for a variety of reasons. Those hacking people call them hackers, this hacking system can also be done through physical access or even through remote access, it is not necessary that the hacking result should be harmed with an aim of destroying one's computer or personal information. But in case if the hacker still checking the information also comes under the cyber crime. Even infiltration comes under cyber crime, there is a provision for punishment. They typically have expert-level skelets in special software programs or languages. There may be many previous intentions of hacking, but the most common are - greed, fame, power etc. Learn the Truth About Hacking In The Next 10 Minutes. The example of hacking s sown as below in the fig. no.-2.

Fig. No.-2 (Hacking)

Sources: Adapted from https://www.cnet.com/news/global-hacking-campaign-targets-critical-infrastructure/ on 13Januray,2019.

Spreading Computer Virus: Cyber criminals send some software to your computer where viruses can be hidden, they contain virus plural such as virus, verms, logic horse, Trojan horse etc. can be harmful to the computer here, when you open someone's site or inappropriate site etc. From an unregistered site or download something, through this the computer gets viruses which results in deleting the data. Also, screwed some programs on the virus takes your line that you do not want as shown in the fig. no.3.

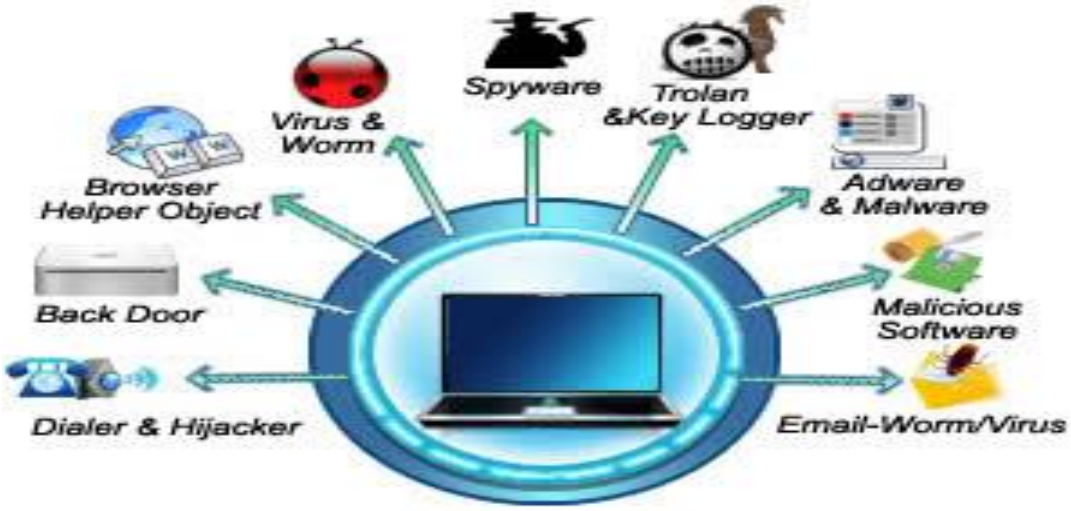

Fig. No.3 (Spreading Computer Virus)

Sources: http://files-recovery.blogspot.com/2011/04/27-malware-types-and-their.html accessed on 13January, 2019.

Theft of FTP Passwords: FTP password theft: This is another common way to tamper with web sites. FTP password hackers take advantage of the fact that many webmasters store their login information on a well-protected PC. Hackers search Victim's system for FTP login details, and then sends them to their remote computer. He then logs on to his web site through his remote PC and modifies the web pages as they like. Virus can be spread in many ways like as shown in the fig. no.4.

Fig. No.4 (Theft of FTP Passwords)

Sources: Adapted from https://www.google.com/search, accessed on 13January, 2019

Virus Dissemination: Virus spread: Computer viruses are a program that infects a system or file. These tend to be broadcast by other networks on the network. They disrupt computer operations and affect store data - either modify it or delete it altogether. The most common reason why one's PC may be infected with viruses or malware Unlike the virus, "Worms" does not need a host. They are still replicated when they do not eat all the available memory in the system. Computer viruses are typically spread through removable media or the

Internet, a flash drive, CD-ROM, magnetic tape or other storage device that is already infected with the virus. Along with this, email attachments, websites or infected software are also vulnerable to viruses. How do you know if your computer is infected with virus or not? When a virus arrives on a PC, then it spreads on all PCs by the network. All computer viruses are due to direct or indirect economic damage. Based on this, two categories of viruses have been created: Those that are only spread and do not cause the intentional damage Those who are programmed to cause the loss. You should use the best anti-spyware and malware software for your PC's security.

Fig. No. 5 (Virus Dissemination)
Sources: Adapted from https://www.google.com/search, accessed on 13January, 2019

Logic Bomb: A logic bomb, also called "slag code", is a malicious code, which is deliberately inserted in software to excel the Málcio Tasc when triggered by a special event. It is not a virus, yet it usually behaves like a virus. It is secretly inserted into a program and it remains inactive until it has a specific condition. They become active in a specific condition. For example, the infamous "Friday the 13th" virus only attacked specific dates; It used to attack the day on which the 13th of the day came on Friday and slow the system down.

Phishing: Phishing is usually done by email spoofing. It looks like this email has come from your back but in fact they are fake. Clicking the link contained in the user is taken to the fake website. Here, whatever information they fill, they go to hackers. How to find out which e-mail is Fake, Spoofed or Spam? Make sure to check whether it is safe before clicking any link included in the e-mail. If you do not check the safety before clicking the link, then you can get into trouble.

Cyber Law In India: For different crimes up to Section 65, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 67C, 68, 69, 70 and Section 71 of 'Information Technology Act, 2000' There is a penalty for up to three to five years of imprisonment.

Constitutional Provisions

- According to the jurisdictional provisions in cyberspace under Information Technology Act, 2000: The discovery of information and communication techniques can be considered as the most important invention of the twentieth century from the point of view of the development of human society. The importance of its use in different areas of social development, especially in the judicial process, cannot be underestimated, because of its judicial process due to its high speed, redemption of many

minor problems, lack of human mistakes, less expensive Can play a key role in making trustworthy Not only this, in the execution of such cases, where the physical presence of all the relevant parties is not mandatory, this can be the best option. The list of charges mentioned under the information technology law is as follows:

- Trying to tamper with computer resources - Section 65
- Trying to hack into the data stored in the computer - Section 66
- Penalty for sending restricted information through communication services - Section 66A
- Provision of penalties for misappropriating information stolen from computer or any other electronic gadget - Section 66b
- Provision of penalties for stealing someone's identity - Section 66
- The provision of penalties for accessing personal data of someone with the help of computer by concealing their identity- Section 66
- The provision of penalties for breaking anybody's privacy - Section 66
- Provision of penalties for cyber terrorism - Section 66F
- Provisions related to the publication of objectionable information- Section 67
- Penalty for publishing or circulating sex or obscene information through electronic means- Section 67A
- Publication or broadcast of such objectionable content from electronic means, in which children are shown in obscene mode - Section 67b
- The provision of penalties for interference or interference by the arbitrators - Section 67C
- Provision regarding making objectionable access to a secure computer-section 70
- Misrepresenting data or data - Section 71
- Provisions related to dissolution of mutual trust and privacy - Section 72A
- The provisions relating to making public the information in violation of contract terms - Section 72A
- Publishing of False Digital Signature-Section 73
- Inspector level police officer in the Information Technology Act of section 78 has the right to investigate these cases.
- Provisions related to cyber crimes in the Indian Penal Code (IPC)
  Send threatening messages through email
  -Section 503 of IPC Sending such messages through email, which leads to libel
  -Section 499 of IPC Use of False Electronic Records
  -Section 463 of IPC Fraudulent Websites or Cyber Fraud-IPC
  -Section 420 Keep an eye on someone's stolen email
  -Section 463 of IPC Web Jacking
  -Section 383 of IPC Incorrect use of email

-Section 500 of IPC selling Medicines Online

-NDPS Act Online Arms Weapons-Sales Arms Act66-F:

- Penalties for Cyber Terrorism: In the cases of cyber terrorism, Section 66-F has been replaced in the Information Technology Act, 2000 for the penal code. If any-

(A) To dissolve India's unity, integrity, security or sovereignty or terrorize its inhabitants- (A). Prevents any authorized person from using the computer or the reason for the stoppage. (B) Forcibly attempting to use any computer without encroachment of authority or its authority. (C) puts a thing like a virus in the computer or tries to put it down, that there is a danger of a danger to the lives of people or the danger of property damage or deliberately disturb the services required for life Whether or not there is a possibility of a bad effect on sensitive information under section 70-(II) Inadvertence of rights or rights, deliberately managed to obtain such information from a computer, which is sensitive to the security of the country or the view of its relations with other countries or any confidential information obtained with this intention Does it have a bad effect on India's security, unity, integrity and sovereignty, its relationship with other countries, public life or ethics, or the like If there is a possibility of contempt or defamation of the courts of the country or it is feared to happen, if any crime is promoted or it is feared, if any foreign nation or group of persons or any other person benefits from such information He can be regarded as an accused of cyber terrorism. (2) If a person is involved in a conspiracy to spread cyber terrorism or to do so, he can be sentenced to life imprisonment. In the third edition of the Advanced Law Lexicon published in 2005, the word Cyberspace is also defined on the same pattern. There is a lot of emphasis on the floating word in electronic means, as it can be accessed from any part of the world. The author further defines the term cyber-theft (cyber theft) in terms of the use of online computer services. In this dictionary, cyber laws have been interpreted in such a way that the area of law, which is related to computers and the Internet, and within its realm comes the intelligible property rights, freedom of speech and uninterrupted access to information.

Suggestions

How to Stop Cyber Crime? Computer users can adopt various techniques to prevent cyber crime

- Computer users should use a firewall to protect their computer from hackers.
- Computer users should install anti-virus software such as McAfee or Norton Anti-Virus.
- Cyber experts have advised that users should purchase only on secure websites. They never give their credit card information to suspicious or strangers.
- Users should develop strong passwords on their accounts, ie, include letters and numbers in a password, and constantly update password and login details.
- Keep track of children and limit their use of the Internet.

- Check the security settings of Facebook, Twitter, YouTube and be careful.
- Keep information safe to avoid hacking. Use encryption for most sensitive files or financial records, create regular back-ups for all important information, and store it in another location.
- Users should be careful when using public Wi-Fi hotspots Avoid operating financial transactions on these networks.
- Users should be careful when giving personal information such as name, address, phone number or financial information on the Internet. Make sure websites are safe.
- Before clicking on a link or an unknown root file, all things should be intelligently analyzed.
- Do not open any email in Inbox. Check the source of the message. If there is any doubt, verify the source. Never reply to emails that give information to them

Since various laws and constitutional provisions have been made in regard to social media. A law has been made to deal with these crimes, but by doing some paddy grains on their behalf, women can avoid these problems and remain active on social media without worry. In this regard, Cyber Security expert Jiten Jain advised "to take care of certain things while on active social media. Here we are talking about: What to do, do not First of all, avoid putting your personal photos on social media". Any one of them can use. If you still want to upload photos, do not publicize your privacy settings on your Facebook account. Keep settings so that your friends can see only your friends or people connected with you. Unaware people did not reach them.

Do not say if cyber attacker asks for money.

Adolescents in cyber crime Image Copywrite iStock

Always keep searching on Google about your name so that you know where your name is coming and what website is coming up.

If you see a name in a wrong place or at such a place you have not given permission, then you can ask to remove it immediately. Do not add strangers to Facebook. There may be disadvantages from doing so many times. Add professional people on LinkedIn, do not join them on Facebook. At the same time, do not put personal photos on Twitter at all. This is not a social networking site, it is a tweeting platform. Such settings can be made on Twitter that people can not follow you without your permission. But, people usually do not do this. By making the settings more private, your account can be more secure. Image Copywrite iStock. Many times you block or block someone's account. The blocked person can not access your account after this, but keep in mind that they can reach you from the second account.

In such a way, before accepting the friend request of another unknown profile, keep this thing in mind. If you get stuck in any problem, do not panic, but let the police know about it. How to know fake account It often happens that a Facebook account is used to photograph a girl, but that account is made by a boy. Similarly, Facebook account is also created with fake names and pictures. Thus, people should focus on

real life more than virtual. But, if it cannot be left entirely, then adopt new approaches to safety. If there is a problem, then you should take legal support.

References

- Adam Leinss, The Effects of Software Piracy on Consumers and Software Developers, Online Available at: http://www.leinss.com/files/piracy.pdf
- David Icove, Karl Seger & William VonStorch, Computer Crime,A Crimefighter's Handbook, 1st Edition August 1995, 2001, O'Reilly & Associates, Online Available at: http://oreilly.com/catalog/crime/chapter/cri_02.html
- Deloitte, Cybercrime: A clear and present danger Combating the fastest growing cyber security threat, Online Available at: http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf
- Hinduja, S. (2003).Trends and Patterns among Online Software Pirates, Ethics and Information Technology 5, 49–63.
- Nicholas Cowdery, Emerging Trends In Cyber Crime, 2008, Online Available at: http://www.odpp.nsw.gov.au/speeches/IAP%20-%2013th%20Annual%20Conference%20-%20New%20Technologies.pdf
- Peter K. Yu, Digital Piracy and the Copyright Response, 2004, Online Available At: http://www.peteryu.com/piracy.pdf
- Talwant Singh, Cyber Law & Information Technology, Online Available at: http://delhicourts.nic.in/CYBER%20LAW.pdf.

On-Line Internet Sources

- https://hi.wikipedia.org
- The Information Technology (Amendment) Act, 2008 http://www.naavi.org/ita_2008/index.htm.
- Types of Cyber Crimes & Cyber Law in India, Prashant Mali, CSIC (http//dgit.in/WCyNDA) .
- http://www.cyberlawsindia.net/
- http://dgit.in/UVeIT8