ISSN: 2456–5474 RNI No.UPBIL/2016/68367 Vol.-6* Issue-3* April- 2021
Innovation The Research Concept

Cybercrimes and its Various Kinds

Paper Submission: 01/04/2021, Date of Acceptance: 15/04/2021, Date of Publication: 25/04/2021

In cyber space, it is the best of time for some and the worst of time for others.These day's cyber crimes have grown. In April 2020, reportedly, there were over 18 million daily malware and phishing emails related to Covid 19 monitored by a single emails provider, In addition to more than 240 million Covid 19 related daily spam messages[1]. Twitter hackers collected $120,000 in full public gaze, while a "ransom ware target in California quality paid 116.4 bitcoin or $1.14 million"[2]

In this Article we will read about cybercrimes and the types of it.

Sanjulata
Assistant Professor,
College Education Department (Law)
Govt.P.G.Law College,
Pali, Rajasthan, India

Keywords: Cyber Space, Spam, Phishing.

Introduction

Cybercrimes means a crime which is done with the help of computer and internet. Cybercrime is an illegal work in which computer is used as a mean or an object or both.

Cybercrime refers to the series of organized crime attacking both cyber space and cyber security. Cyber crime refers to criminal activity which is done by individual or organized group using computers and the Internet, technical Gazettes, cell phones. It also involves illegal access (unauthorized access, transmissions of computer data, to from or within a computer system. Cyber criminals use weakness of cyberspace in doing cybercrimes. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet[3].

Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the internet to steal personal information from other users. Day by day tendency and possibilities of cybercrimes is increasing

The History of Cybercrime

In 1970s, criminals committed crimes via telephone lines. The perpetrators were called Phreakers and discovered that the telephone system in America functioned on the basis of certain tones. They were going to imitate these tones to make free calls.John Draper was a well-known Phreaker who worked on it daily; Steve Jobs and Steve Wozniak were inspired by this man, and even joined him. Of course they all ended up on the right path: Steve Jobs and Wozniak founded Apple, the well-known computer company. Actually real cyber crimes started in the year 1981. Ian Murphy was the first man, who was found guilty of Cybercrime in the year 1981. He hacked the American telephone company to manipulate its internal clock, so that users could still make free calls at peak times.Nowadays, online banking is very popular, and that also carries a big risk. For example, hackers can copy log-in codes and names, or retrieve passwords from credit cards and bank accounts. The result is that one can just empty accounts or make purchases online with someone else's account.[4]

Causes of Cybercrime

Following are the Causes of Cybercrimes

Easy to Access

Hackers can steal access codes, retina images, advanced voice recorders, etc. that can fool biometric systems easily and bypass firewalls can be utilized to get past many security systems.

Capacity to store data in Comparatively Small Space

The computer has the unique characteristic of storing data in a very small space. This makes it a lot easier for the people to steal data from any other storage and use it for their own profit.

Complex

The computers run on operating systems and these operating systems are programmed of millions of codes. The human mind is imperfect, so they can do mistakes at any stage. Cybercriminals take advantage of these gaps.

Negligence

Due to negligence there may be a possibility that protecting the computer system we may make any negligence which provides cyber-criminal access and control over the computer system.

Loss of Evidence

The data related to the crime can be easily destroyed. So, Loss of evidence has become a very common & obvious problem which encourages criminal to do cyber crime.[5]

Various Types of Cybercrime

There is much kind of cybercrimes that cybercriminals do.

Malware

This system is used to interrupt computer operations, gather sensitive information, gain access to personal computer system. It may be in the form of any code, script, active ingredients and any software.

Ransomware

Ransom ware is a destructive malware based attacks. It enters in computer network and encrypts files and information through public key encryption.

Hacking

Hacking involves the partial or complete acquisition of certain functions within a system, network, or website. It also aims to access to important data and information, breaching privacy. Most hackers attack corporate and government accounts. There are different types of hacking methods and procedures.

Virus Dissemination

Virus Dissemination is a process. A process in which malicious software destroys the system of the victim. They delete or modify the stored data.

Spoofing

Spoofing is a type of scam in which criminals' attempts to obtain someone's personal information by pretending to be a legitimate business, a neighbour, or some other innocent party. There are several kinds of spoofing, including email spoofing, text message spoofing, caller ID spoofing, and URL and GPS spoofing. In short, if there's a form of online communication, spoofers are trying to scam their way into it—and into your identity and your assets.[6]

Phishing Gathering Information of Password and Details of Credit Card by fraud, Winning Trust and receiving Username through Electronic Communication is called Fishing

"Phish" is pronounced just like it's spelled, which is to say like the word "fish" — the analogy is of an angler throwing a baited hook out there (the phishing email) and hoping you bite. The term arose in the mid-1990s among hackers aiming to trick AOL users into giving up their login information. The "ph" is part of a tradition of whimsical hacker spelling, and was probably influenced by the term "phreaking," short for "phone phreaking," an early form of hacking that involved playing sound tones into telephone handsets to get free phone calls.[7]

Email Bombing and Spamming

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack. This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters. "Spamming" is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead you to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receivethe reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users' address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses.Sending spam violates the acceptable use policy (AUP) of almost all internet service providers. If your system suddenly becomes sluggish (email loads slowly or doesn't appear to be sent or received), the reason may be that your mailer is processing a large number of messages. Unfortunately, at this time, there's no way to completely prevent email bombing and spam mails as it's impossible to predict the origin of the next attack. [8]

Web Jacking

Web Jacking term is derived from the hi jacking. In this crime, criminals (hackers) take control over another's website. They do it fraudulently. He may change the information of another's site. In this crime the owner of the website has no more control on his own website and hackers use this website for his own interests.

Cyber Stalking

Cyber Stalking is also a Cybercrime. In this crime Internet or other electronic means are used to stalk or harass anybody. Defamation, slender and libel may be including in it. This crime mainly happens against women.

Types of Cyber Stalking

There are three most common forms of cyber stalking:

Email Stalking

Sending hate, obscene, or threatening emails, or sending viruses and spam. Only considered to be stalking if this is done in repletion manner.

Eerily similar to physical stalking which would include sending hate mail through the postal service.

Internet Stalking

Spreading rumors or tracking victims on the web.Spreading rumors takes on a public form of harassment versus a private approach.

The aim of spreading rumors would be to slander the victim. Tracking victims can be done in without the victim ever knowing they are being watched.

Computer Stalking

Hacking into a victim's computer and taking control of it. This takes a high level of computer knowledge but instructions can be found online.

The invader is able to control the actions of the victim's computer whenever that computer is connected to the internet.[9]

Data diddling

In data diddling attack an attackers change the information in a database. He gains access to the database. He modifies data in the database. Forgery, mis representation is examples of data diddling.

Credit Card Fraud

Credit card fraud term is used to obtain money or goods fraudulently. It may be happened when credit card number is given to unfamiliar or credit card stolen.

Salami Slicing Attacks

A salami attack is when small attacks add up to one major attack that can go undetected due to the nature of this type of cyber crime. It also known as salami slicing. Although salami slicing is often used to carry out illegal activities, it is only a strategy for gaining an advantage over time by accumulating it in small increments, so it can be used in perfectly legal ways as well .The attacker uses an online database to seize the information of customers that is bank/credit card details deducting very little amounts from every account over a period of time. The customers remain unaware of the slicing and hence no complaint is launched thus keeping the hacker away from detection.[10]

Software Piracy

Software piracy is the unauthorized use, copying or distribution of copyrighted software. It may take many forms, including:

Unauthorized copying of software programs purchased legitimately, sometimes known as "end-user" piracy[11]

Section 63B: Knowing use of infringing copy of computer programme to be an offence: Any person who knowingly makes use on a computer of an infringing copy of a computer programme shall be punishable with imprisonment for a term which shall not be less than seven days but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees.[12]

Others

Another examples of cyber crime are cyber pornography, cyber bullying. Pornography specifically child pornography is a serious crime. Pornography includes text, photos, videos content and audio which are sexual in nature. This is based on sexual acts and nudity. Publishing such materials electronically is punishable under IT (Amendment) Act 2008, sec 67(A), IPC sec 292, 293,294 ,500 506 and 509.

Aim of the study

To make people aware about cybercrimes and its types.

Conclusion

Crimes that are committed with the help of electronic devices like computers, smartphones, tablets which are connected to the internet, are called cyber crimes. Cyber crimes are serious crimes. These crimes are easy to do through the internet apart of traditional crimes. These crimes affect a large area in a short period of time. Many laws are there in India to fight with these crimes like IT Act 2000, IPC, 1860 etc. If any person becomes victim of any Cybercrime he should take help of police. But it is very difficult to find out or catch the cybercriminals, jurisdiction problems are also faced by the court in these crimes so it is better to be careful. No one should share their personal information like password, OTP with strangers, should not open emails that comes from unknown persons.

References

1. *https://cloud.google.com/blog//product/identity-security/protecting-against-cyber-threats-during-covid19-and-beyond*
2. *Article, Syed Akbaruddin, last updated on 30 July 2020, A quest for order amid cyber insecurity, https://www.thehindu.com/opinion/lead/a-quest-for-order-amid-cyber-insecurity/article32225383.ece*
3. *https://techterm.com/definition/cybercrime#:~:text=Cybercrime%20also%20includes%20non%2Dmonetary,business%20information%20on%20the%20Internet.&text=Both%20of%20these%20methods%20lure,asked%20to%20enter%20personal%20information*
4. *https://goosevpn.com/blog/origin-cybercrime*
5. *https://lecturernotes.in/project-report/17568-cyber-crime-and-its-prevention/12*
6. *https://www.investopedia.com/terms/s/spoofing.asp.*
7. *https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html*
8. *http://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html*
9. *https://sites.google.com/site/onlineriskthecyberstalker/types-of-cyberstalking*
10. *https://ajmaurya.wordpress.com/2014/03/27/what-is-a-salami-attack/*
11. *https://www.ptc.com/en/documents/software-piracy/faq#:~:text=Software%20piracy%20is%20the%20unauthorized,as%20%22end%2Duser%22%20piracy*
12. *https://indiankanoon.org/doc/37620088/#:~:text=be%20an%20offence.,%E2%80%94Any%20person%20who%20knowingly%20makes%20use%20on%20a%20computer%20of,may%20extend%20to%20two%20lakh*