ISSN 2582 - 211X

LEX RESEARCH HUB JOURNAL

On Law & Multidiciplinary Issues

Email - journal@lexresearchhub.com

VOLUME II, ISSUE II
JAN - MARCH, 2021

https://journal.lexresearchhub.com

Lex Research Hub Publications

DISCLAIMER

EDITORIAL BOARD

Assistant Editors

ABOUT US

Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X) is an Online Journal is quarterly, Peer Review, Academic Journal, published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essays in the field of Law and Multidisciplinary issues.

Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X) welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

CYBERCRIME, CLASSIFICATION & IT'S PREVENTION

Author –

Sonam Singh

Student (B.B.A LLB)

Amity University, Patna

ABSTRACT

Cyber crime conjointly referred to as digital crime, any crime that involves a telecommunication device and a network. As user and businesses increase by technology, they're exposed to the growing law-breaking threats. victimization the computers for our regular transactions is kind of common in a day. as an example, we tend to pay our insurance premium, bills, flight train or bus tickets, order book or the other product digital victimization computer, mobile phones, public browsing centers etc. Most of users doing on-line transactions as growing speedily ever since, due to the convenience it provides to the user to interact business while not being physically gift within the space wherever the group action happens. Criminals committing law-breaking are growing day-by-day with the enhanced range of users doing on-line transactions. law-breaking covers a large vary of various attacks like Cyber stalking, Cyber terrorism, spreading viruses or installation of Malware, net fraud, Spamming, Phishing, porno graphics and holding rights violation etc.

Keywords - crime, technology, terrorism, smart phones

INTRODUCTION –

In common words the "cyber crime" is that the crime, criminality or any illegal activity done by a person via a use of any digital telecommunication networks like web, mobile phone or lap top, etc are term as cyber crime.[1]The word cyber crime isn't outlined in any act, presumptively as a result of at the time of prescribing constitution there wasn't any digital platform like web, internet, etc. Exchanging or spreading fake messages with an aim of disturbing the privacy of a person or trying to threaten national security through internet or by use of any social media.

HOW CYBER CRIME IS DONE –

Cyber crime is done by exploits the software system or by hack the cryptography or programming from a system. The assailant main target to hacked or use the network by their own provision.

[1] https//:{www.britanica.com/cybercrime- means-its}classification

WHY CYBER CRIME HAPPENS-

Alternative crimes like murder, theft, kidnapping ,etc needs very little measure to execute that further more as they need to appeared as a physical type however in contrast to alternative crime cyber needn't be physically or expenses cash to commit the soul issue would like might be a sensible information of programming.

CLASSIFICATION OF CYBER CRIME –

1. Cyber stalking

2. Cyber coercion (cyber terrorism)

3. Cyber vandalism

4. Hacking

5. Phi sing

6. Pornography

1) Cyber stalking - It's a kind of crime during which the assailant harasses a victim by victimization digital platform or by social networking site like Face book, Email, any web site.

- They aim specific victim inside treating messages.
- It is that the real world stalking incident just one distinction is that it's done by use web.

Precaution that we should always follow to shield from cyber stalking-

a) Use primary email account just for communication with folks to whom you trust
b) Set filtering change in your email to prevent delivery of unwanted message
c) Do not place any identifying details in your social networking platform
d) Invariably keep of social networking information processing system in a very privacy mode.

2) Cyber act of terrorism (cyber terrorism)[2] - It suggests that any violence created on the web by victimization, on portable, computer or any digital platform it will end as cyber terrorism. Cyber terrorist act is also called as "electronic terrorism". The essential focus of cyber terrorist is business, installation, and power plants. The target is not a personal they regularly target a mass.

Punishment for cyber terrorist act.–

(1) whoever[3],–

(A) With intent to threaten the unity, integrity, security or sovereignty of Asian nation or to strike terror within the people or any section of the people by –

(i) Denying or cause the denial of access to a person licensed to use system resource.

(ii) Trying to penetrate or access a system resource while not authorization or exceptional licensed access.

(iii) Introducing or inflicting to introduce any system.

(B) Wittingly or deliberately penetrates or accesses a system resource while not authorization or exceptional licensed access and by suggests that of such conduct obtains access to information knowledge or system knowledge base that's restricted for reasons of protect the State or foreign relations or any restricted info knowledge or system knowledge base, with reasons to believe that such info, knowledge or system knowledge base thus obtained could also be wont to cause or possible to cause injury to the interests of the sovereignty and integrity of Asian nation, protect the State, friendly relations with foreign States, public order, decency or morality or in relevance contempt of court, defamation or incitement to Associate in offence or to the advantage of any foreign nation, cluster of people or otherwise commits offence of cyber terrorist act.

(2) Whoever commits or conspires to commit cyber terrorist act shall be punishable with imprisonment which could extend for all times.

[2] http://nti.org/about/cyber-terrorism
[3] https://indiacode.nic.in>punishment for-cyber-terrorism

3) Cyber vandalism-[4] It Implies that "to hurt or destroy the alternative property" once assaults destroying dangerous information rather that stealing or misusing them it will consider as cyber vandalism.

Two kinds of vandalism are -:

A. Website defacement

B. Creation of Malware

A) Website defacement - The word defacement implies that to spoil or destroy. Website defacement means that the method to spoil or harm the web site by an assailant or to ascertain the other look in website and management by assailant method is finished by to gaining on unauthorized legal hacking.

B) Creation of Malware- Malware it's the software system that is meant for the aim of damage| and to harm the computer. Creation of Malware- The software system advisedly styles by a bunch vary of individual's agency for hack or blackmails.

4) Hacking- The unauthorized user who breaks the computer system by change destroy or steal the information often by installing hazardous malware without the consent or knowledge of user.

Punishment for dishonestly receiving stolen computer resource or communication (hacking) –

Whoever deceitfully receive or retains any taken system resource or communication devise knowing or having reason to believe a similar to purloined system resource or communication device, shall be penalized with imprisonment of either description for a term which can reach 3 years or with fine which can reach rupees 1 lakh or with both.

5) Phi sing - The process in which the hackers caught and formation by send a link on email by messages or by any social network it's consider as phi sing. The motive of hackers to got the tale

[4] The cyber wire .com/you tube slide – presentation.

of debit Card, password, credit card, etc. Protect yourself from phishing by Check spelling of URL addresses.

6) Pornography - In simple word its define as the act of using cyberspace to create display an import or publish any obscene material.

- Viewing pornography is legal in India; downloading such content does not amount to an offence.
- Publication of pornographic content online is illegal
- To store cyber pornographic is not an offence.

Punishment for pornography-

Whoever publishes or transmits or causes to revealed or transmitted within the electronic type any material that has sexually specific act or conduct shall be penalized on 1st conviction with imprisonment of either description for a term which can reach 5 years and with fine which can reach 1000000 rupees and within the event of second or resultant conviction with imprisonment of either description for a term which can reach seven years and conjointly with fine which can reach 1000000 rupees. number of cyber crimes as well as there are many provisions in the IPC and IT act that imbricate each other.

HOW TO FILE CYBER CRIME CASE[5] –

The cybercrime complaints can be registered with the cybercrime cells. We can file complaint in online or offline method. Person can choose by their own convenience. It's not mandatory for a person to file a complaint in which they resident or where the crime occurred because the jurisdiction of cyber cells is global jurisdiction i.e., the cyber crime complaint can be filed any of cyber cells which have been established in our country.

[5] https://blog.ipleaders.in/procedure for filing cybercrime-complaint-in-India/amp

However, if a person does not have idea of cyber cells he or she may lodge a FIR at the local police station.

Documents required for filling an FIR at police station

- Name, contact, Address proof
- A screenshot of URL
- Content in the form of hard & soft copies.

Government facilitates a online complain for this where you can easily filled your complain (https://cybercrime.gov.in/Default.aspx)

PRECAUTIONS WE SHOULD FOLLOW TO SAFEGUARD AGAINST CYBERCRIME-:[6]

- Keep software system and software package updated.
- Keeping your software system and OS up thus far ensures that you just get pleasure from the latest security patches to safeguard your system.
- Use anti-virus software system and keep updated
- .Never open attachments in spam emails.

.

- Do not click on links in spam emails or entrusted websites.
- Another manner of us become victims of transgression is by clicking on links in spam emails or different messages, or unacquainted websites.
- Avoid doing this to stay safe on-line.
- Do not provide out personal information unless secure.

[6] Kaspersky.co.in {how to protect c}

CONCLUSION

In today's era, it has been seen the threat of digital crime isn't as massive because the authority claim. This implies that the tactic that they introducing to combat it represents an unwarranted attack on human rights and isn't proportionate to the threat exhibit by cyber-criminals. A part of the matter is that there aren't any reliable statistics on the problem; this implies that it's arduous to justify the enhanced powers that the Regulation of inquiring Powers Act has given to the authorities. These powers will be ineffective in addressing situation of digital system.