Websites:
http://www.sciencepub.net
http://www.sciencepub.net/researcher

Emails:
editor@sciencepub.net
marslandresearcher@gmail.com

Researcher

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

The Role of Cyber Law in Cyber Security in India

Ajay Panchal

H. No. 752/05, Urban Estate, Kurukshetra University, Kurukshetra, Haryana (India)
E-mail- ajaypanchalw@gmail.com

Abstract: Cybercrime is crime which occurs when there is any kind of illegal or unauthorised activity which takes access of your data or access which involves any kind of computer or any such kind of devices. In recent times, there has been a rapid increase in cybercrime all over the world. Cybercrimes also include fraud, abuse, as well as the misuse of devices. As in these times, the internet is being used in almost all the sectors for all kind of work and with this usage in every field it has given a vast scope to the cyber criminals to use any kind of data be it in the field of sports or some personal information of the people. The main aspect of this cybercrime is that they don't even have to be physically present to commit the crime.

[Panchal, A. **The Role of Cyber Law in Cyber Security in India.** *Researcher* 2023;15(4):1-5]. ISSN 1553-9865 (print); ISSN 2163-8950 (online). http://www.sciencepub.net/researcher. 01.doi:10.7537/marsrsj150423.01.

Keywords: Cyber crime, Hacking, Phishing, Vishing, Cyber squatting

Introduction:

As the world becomes increasingly digitized and cloud-based, the technology and computer industries continue expanding and transforming. Technology is now embedded in business and consumer affairs, leading to a prevalence of information leaks, data breaches, and outright assaults by hackers and other cybercriminals. The old adage "the best defence is a good offense" holds true in computer-related fields. Keeping users, networks, and the cloud safe from cybercriminals is increasingly important as attackers become more sophisticated.

Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual properly. Cyber crime in the context of national security may involve activism, traditional espionage, or information warfare and related activities.

The invention of Computer has made the life of humans easier, it has been using for various purposes starting from the individual to large organizations across the globe. In simple term we can define computer as the machine that can stores and manipulate/process information or instruction that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other's benefit since decades [1]. This gave birth to "Cyber Crime". This had led to the engagement in activities which are illegal to the society. We can define Cyber Crime as the crimes committed using computers or computer network and are usually take place over the cyber space especially the Internet [2]. Now comes the term "Cyber Law". It doesn't have a fixed definition, but in a simple term we can defined it as the law that governs the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc are comprehended by the Cyber Law [3]. The UN's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL) Model [4].

First, we should understand what cyber laws are. The laws that prevail in cyberspace and protect the data are known as cyber laws. All the sources that are found on the internet are found in cyberspace. The most common source which protects cyberspace is the Information Technology Laws, 2000. The main purpose of this act is to provide legal protection to electronic commerce and to facilitate all the records that are in the hands of the government. Cybercrimes are those illegal acts that include hacking and stealing the data found on the internet be it online shopping, online transactions etc. sometimes I also think that whether my data, my details are safe or not. And to answer this question has a very big answer that is NO. Data protection aims to give us privacy rights in the interest of the public to protect these details. Our data is completely in danger zone but just to make those hackers stay in fear and to make our details safe on the

internet various acts are formed by the governments of various countries according to their laws and rights. We saw a very common example of 'the boy's locker room' where all the underage boys were sharing pictures of underage girls and were talking terrible things about them. They also made rape threats to them and their cyber security were endangered during the times. As we all know that the entire world is on the internet now. From a kid to an old person everyone knows how to operate the internet and all the details are open on the internet. For example, Aadhaar card details, passport forms, bank account details etc.

Cyber Stalking Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property [2]. Cyber stalking is a technologically-based "attack" on one person who has been targeted specifically for that attack for reasons of anger, revenge or control. Cyber stalking can take many forms, including: o

- harassment, embarrassment and humiliation of the victim
- emptying bank accounts or other economic control such as ruining the victim's credit score
- harassing family, friends and employers to isolate the victim The term can also apply to a "traditional" stalker who uses technology to trace and locate their victim and their movements more easily (e.g. using Facebook notifications to know what party they are attending). A true cyber stalker's intent is to harm their intended victim using the anonymity and untraceable distance of technology. In many situations, the victims never discover the identity of the cyber stalkers who hurt them, despite their lives being completely upended by the perpetrator.

History of Cyber Crime The first Cyber Crime was recorded within the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage's analytical engine is considered as the time of present day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that t the new technology cannot be utilized in the future [7].

Hacking

"Hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37 per cent increase this year. A case of suspected hacking of certain web portals and obtaining the residential addresses from the e-mail accounts of city residents had recently come to light [3]. Crackers are people who try to gain unauthorised access to computers. This is normally done through the use of a 'backdoor' program installed on your machine. A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer. Obviously, a good protection from this is to change passwords regularly. In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking [9]. The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on the Internet and other networks. M.I.T. engineers in the 1950s and 1960s first popularized the term and concept of hacking. Starting at the model train club and later in the mainframe computer rooms, the so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities. Later, outside of M.I.T., others began applying the term to less honorable pursuits. Before the Internet became popular, for example, several hackers in the U.S. experimented with methods to modify telephones for making free long-distance calls over the phone network illegally. As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hackers and hacking.

Phishing

Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. 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 remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account [4]. Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate

enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately. Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting [8].

Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well known and trustworthy Web sites. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online. A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait. Phishers use a number of different social engineering and e-mail spoofing ploys to try to trick their victims.

Cross Site Scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls. Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites [7]. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it. An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by your browser and used with that site. These scripts can even rewrite the content of the HTML page.

Vishing

One emerging threat called vishing has already affected thousands of people in the Midwest. In these cases, criminals use the power of Voice over Internet Protocol to spoof caller IDs and prey on unsuspecting financial institution customers. Believing the information displayed on their caller IDs is accurate, customers are willing to share their private personal and financial information with the caller who is not, as their caller ID claims, a financial institution employee [5]. Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless. Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with.

Bot Networks

A cyber crime called 'Bot Networks', wherein spamsters and other perpetrators of cyber crimes remotely take control of computers without the users realizing it, is increasing at an alarming rate. Computers get linked to Bot Networks when users unknowingly download malicious codes such as Trojan horse sent as e-mai l attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them get activated, and those who are behind the Bot Neworks attacks get the computing powers of thousands of systems at their disposal [6]. Attackers often coordinate large groups of Bot-controlled systems, or

Bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. Trojan horse provides a backdoor to the computers acquired. A 'backdoor" is a method of bypassing normal authentication, or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program, or could be a modification to a legitimate program. Bot networks create unique problems for organisations because they can be remotely upgraded with new exploits very quickly and this could help attackers pre-empt security efforts. In a first of its kind initiative in India to tackle cyber crime, police have taken the initiative to keep an electronic eye on the users of the various cyber cafes spread over the city. The Kerala State IT Mission has launched a Web portal and a call centre to tackle cyber crime. [The Hindu Business line, Tuesday, Jul 31, 2007]. The Central Bureau of Investigation (CBI) and the Mumbai police have recommended issuance of licenses to cyber cafe owners. Many countries, including India, have established Computer Emergency Response Teams (CERTs) with an objective to coordinate and respond during major security incidents/events. These organisations identify and address existing and potential threats and vulnerabilities in the system and coordinate with stakeholders to address these threats. Policy initiatives on cyber crime are as yet lethargic because of a general sense that it is nothing more than juvenile hackers out to have fun or impress someone. Prateek Bhargava, cyber law expert says, "There is huge potential for damage to national security through cyber attacks. The internet is a means for money laundering and funding terrorist attacks in an organized manner.

The Role of Cyber Laws in Cybersecurity

Cybersecurity and information protection have become the buzzwords of today's post-pandemic world. Organizations, governments, financial institutions, and other entities remain under constant cyber threats. The means of cyberattacks that are executed by cybercriminals are getting more sophisticated with each passing day, thereby increasing the risk of any major cyber security breach. Therefore, it has become indispensable for organizations that they understand cyber laws and legal nuances of cybersecurity.

Did you know! According to Forbes, in the year 2019, both individuals and business organizations lost over $3.5 billion because of cybercrime. In this period, a staggering 467,361 cybercrime complaints were registered by the Federal Bureau of Investigation (FBI).

In this blog, we will understand about the utility of cyber laws and discuss EC-Council University's dedicated course on cyber laws included in its Master of Science in Cyber Security degree and a course dedicated to legal issues in cybersecurity in its Bachelor of Science in Cyber Security degree.

CYBER SECURITY DURING COVID ERA

Since the end of 2019, most nations have started to work from home, doing all their work online. Even I attend all the webinars, my college events, and classes on the internet. This obviously needed our information. All these things were openly filled on the internet. All the payments were done through online transactions which required our bank details, that were also exposed in the market. All the details were and are still on the internet and we are not sure when and how they will get hacked by anyone. The government has mode the following acts just to ensure our privacy and data protection: –

- **Information technology act, 2000**: In our country the cyber laws are mostly governed by the information technology act, 2000. This act provides a legal inclusiveness to electronic commerce and facilitates registration of real time records with the government. Cybercrimes have been growing for a few years; therefore, a number of amendments were made to protect the data from getting hacked. The IT act that was enacted by the parliament highlights the painful punishments and penalties that are put on those who do these crimes for safeguarding the e-commerce, e-banking and e-governance sectors. This act guides the Indian legislation to govern cyber-crimes in a more efficient way.
- **Indian penal code,1980:** cybercrimes also include many criminal activities like theft, fraud, defamation and mischief and all these activities come within the sector of the Indian penal code and are subject to the provisions under the Indian penal code. The Indian penal code therefore makes sures these thefts and associated cyber frauds, invoked along with the information technology act, 2000. All the Relevant sections include section 464, 468,465,471,469.
- **NIST Compliance:** The cyber-security framework authorized by the national institute of standards and technology (NIST) has established this sector as the most reliable global body by offering an easy approach to improve cyber-security. The NIST cyber-security framework encompasses all the required guidelines, standards and practices

that are best to manage the cyber related risks in a responsible manner. This framework makes the main priority for flexibility and cost effectiveness.

Conclusion: The internet is the most important part of our daily lives now. Everything we do is on the internet exposed to the entire world. Be it social media, our own bank details, college details etc. we are always in danger. Those who hack and do all these cybercrimes should be afraid of the laws that are being made by law and it should be executed in a way that every little detail of the person is protected. It is practically now possible to completely stop all these cybercrimes but we can at least have a back that we can take to take a stand for ourselves in times of trouble. If the internet has made our lives easy, it has also made a very difficult situation if it is done for illegal matters. So, the government should work on the new laws and amendments by considering the modern techniques that the new hackers use to do all these crimes.

References:

[1] Roderic Broadhurst and Peter Grabosky, "Cyber Crime – The Challenges in Asia", Hong Kong University Prees, 2005. ISBN: 962-209-724-3.
[2] Paul Bocij, "Cyber Stalking - Harassment in the Internet age and How to protect your family" Library of Congress Cataloging-in-Publication Data, 2004. ISBN:0-275-98118-5.
[3] Jon Erickson, "Hacking – The Art of Exploitation", William Pollock Publishers, 2nd Edition, 2008. ISBN: 1-59327-144-1
[4] H. Thomas Milhorn, "Cyber Crime – How to Avoid Beconing a Victim", Universal Publishers, 2007. ISBN: 1-58112-954-8.
[5] Markus Jacobsson and Zulfikar Ramzan, "Crime Ware- Understaning New Attacks and Defenses", Symantec Press.
[6] Gray Byrne, "Botnets – The Killer Web App", Syngress Publishing Inc., ISBN: 1-59749-135- 7.
[7] Peter Stavroulakis and Mark Stamp, "Handbook of Information and Communication", Springer. E-ISBN : 978-3-642-04117-4. ISBN: 978-3-642-04116-7.
[8] Mark Stamp, "Information Security – Principles and Practices", John Wiley & Sons Inc,. ISBN: 978-0-470-62639-9.
[9] Giorgio Franceschetti and Marina Grossi, "Homeland Security – Technology Challenges from sensing and Encrypting to mining and Modeling", Library of Congress, US. ISBN: 978-59693- 289-0.

3/16/2023