IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

A Contemplation of Cybercrime: A Global Issue

Prof. Saquib Ahmad Khan
Research Scholar: Shri.J.J.T.University
Assistant Professor: Sinhgad College of Commerce

ABSTRACT:
As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cyber-crimes. While law enforcement agencies are trying to tackle this problem, it is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid being a victim of cyber-crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet. Cybercrimes are responsible for the interruption of normal computer functions and has been known to cause the downfall of many companies and personal entities. This research paper aims to discuss following aspects of Cybercrimes: the definition, why they occur, laws governing them, methods of committing cybercrimes, who they affect, and cybercrime prevention procedures. This paper will report will display statistical data which will give an idea of how far cybercrimes has increase over the period of ten years or more.

KEYWORDS: Cybercrimes, theft, hacking, cyber world, malicious.

I. INTRODUCTION:

Cyber criminals use internet and computer technology to hack user's personal computers, smart phone data, and personal details from social media, business secrets, national secrets etc. Criminals who perform these illegal activities through the internet are called – Hackers. Though law enforcement agencies are trying to tackle this problem, it is growing regularly and many people have become victims of identity theft, hacking and malicious software. One of the best ways to stop these criminals and protect sensitive information is by making use of inscrutable security that uses a unified system of software and hardware to authenticate any information that is accessed over the Internet. Let's find out more about cyber-crimes.

II. LITERATURE REVIEW:

2.1. Kanika Chhabra and Gunjan Chhabra (2015):

The authors of this article claim that there are many laws and measures that have been framed and have been taken to prevent these evils, such as IT ACT 2000, National Policy on Cyber Security, etc. Although the term cyber-crime has no origin or reference point in the law and also activities such as cyber vandalism, cyber violence and cyber rape are not classified and have a legal status in the cyber-crime context. This document focuses primarily on the challenges in cyberspace and highlights the urgent need to reform the Indian cyber edict framework and several issues that are lacking in cyber law enforcement.

2.2. Jigar Shah (2016):

In India, every minute a person becomes an Internet user. Its convergence with digitally supported platforms and devices, safeguarding parents and students from cybercrime is becoming a difficult task. Furthermore, the reality is that Internet users do not update on vulnerable cyber threats and security problems, since they update themselves with the use of Internet-enabled tools and applications. This research work focuses on finding out if citizens are truly aware that he / she is vulnerable to various cybercrimes and what measures can be taken to make the citizen more aware and updated. The document suggested a conceptual model that explains how to maintain and implement cybercrime awareness programs among Internet users.

III. OBJECTIVE:

1) To study and know the concepts and causes of cyber-crime.
2) To understand the common types of cybercrimes.
3) To learn how tackle these cyber-crimes.
4) To learn the initiative taken by Government of India to control cybercrime.

3.1. TYPES OF CYBER CRIME:

There are many types of cyber-crimes and the most common ones are explained below:

- **Hacking:** It is a simple term that defines sending an illegal instruction to any other computer or network. In this case, a person's computer is hacked so that his personal or sensitive information can be accessed. The criminal uses a variety of software to crack a person's computer and the person may not be aware that his computer has been accessed from a remote location. Often, government websites are a hot target for hackers because it helps them gain notoriety which is further fuelled by aggressive media coverage. This is different from ethical hacking which is used by many organizations to check their Internet security protection.
- **Child pornography and Abuse:** The internet is being highly used to abuse children sexually worldwide. This is also a type of cyber-crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The Cyber security department of every nation is spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.
- **Piracy or Theft**: This crime occurs when a person violates copyrights and downloads music, movies, games, and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the judicial system is addressing this cyber-crime and there are laws that prevent people from illegal downloading. Film producers and directors often become victims of this crime.
- **Cyber Stalking**: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.
- **Cyber Terrorism:** Cyber terrorism, also known as information wars, can be defined as any act of Internet terrorism which includes deliberate and large-scale attacks and disruptions of computer networks using computer viruses, or physical attacks using malware, to attack individuals, governments and organizations. The goal of terrorism is to create a feeling of terror in the minds of the victims. Keeping this concept in mind, it becomes easier to differentiate cyber-attacks for a financial, or egotistical, gain from acts of cyber terrorism. Cyber terrorists operate with the goal of damage and destruction at the forefront of their activities.
- **Identity Theft**: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber-crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.
- **Computer vandalism:** Computer vandalism is a type of malicious behavior that involves damages computers and data in various ways and potentially disrupting businesses. Typical computer vandalism involves the creation of malicious programs designed to perform harmful tasks such as erasing hard drive data or extracting login credentials. Computer vandalism differs from viruses, which attach themselves to existing programs.
- **Malicious Software**: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

3.2. CAUSES OF CYBER CRIME:

Cyber criminals always opt an easy way to make big money. They target rich people or rich organizations like banks, casinos and financial firms where a huge amount of money flows daily and hack sensitive information. Catching such criminals is difficult. Hence, that increases the number of cyber-crimes across the globe.
Computers are vulnerable, so laws are required to protect and safeguard them against cyber criminals.

We could list following reasons for the vulnerability of computers:

- **Easy to access** – The problem behind safeguarding a computer system from unauthorized access is that there are many possibilities of breach due to the complex technology. 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 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. The cyber criminals take advantage of these gaps.
- **Negligence** – Negligence is one of the characteristics in human conduct. So, there may be a possibility that protecting the computer system we may make any negligence which provides a cyber-criminal the 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 paralyzes the system behind the investigation of cyber-crime.

3.3. HOW TO TACKLE CYBER CRIME:

To tackle cybercrime effectively, establish multidimensional public-private collaborations between law enforcement agencies, the information technology industry, information security organizations, internet companies and financial institutions. Unlike the real world, Cyber criminals do not fight one another for supremacy or control. Instead, they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals.

The best way to go about is using the solutions provided by Cross-Domain Solutions. This allows organizations to use a unified system comprising of software and hardware that authenticates both manual and automatic transfer and access of information when it takes places between different security classification levels. This allows seamless sharing and access of information within a specific security classification, but cannot be intercepted by or advertently revealed to the user who is not part of the security classification. This helps to keep the network and the systems using the network safe.

- **Use Strong Passwords:** Use the different password and username combinations for different accounts and resist the temptation to write them down.
- **Be social media savvy:** Be sure to keep your social networking profiles (Facebook, Twitter, YouTube, etc.) are set to private. Be sure to check your security settings. Be careful of what information you post online. Once it is on the Internet it is there forever.
- **Secure your Mobile Devices:** Many people are not aware that their mobile devices are also vulnerable to malicious software, such as computer viruses and hackers. Be sure to download applications only from trusted sources. It is also crucial that you keep your operating system up-to-date. Be sure to install anti-virus software and to use a secure lock screen as well. Otherwise, anyone can access all your personal information on your phone if you misplace it or even set it down for a few moments. Someone could even install malicious software that could track your every movement through your GPS.
- **Protect your data:** Protect your data by using encryption for your most sensitive files such financial records and tax returns.
- **Protect your identity online:** When it comes to protecting your identity online it is better to be too cautious than not cautious enough. It is critical that you be cautious when giving out personal ID such as your name, address, phone number and/or financial information on the Internet. Be certain to make sure websites are secure when making online purchases, etc. This includes enabling your privacy settings when using/accessing social networking sites.
- **Keep your computer current with the latest patches and updates:** One of the best ways to keep attackers away from your computer is to apply patches and other software fixes when they become available. By regularly updating your computer, you block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to break into your system.
- **Protect your computer with security software:** Several types of security software are necessary for basic online security. Security software essentials include firewall and antivirus programs. A firewall is usually your computer's first line of defense. It controls who and what can communicate with your computer online. You could think of a firewall as a sort of "policeman" that watches all the data attempting to flow in and out of your computer on the Internet, allowing communications that it knows are safe and blocking "bad" traffic such as attacks from ever reaching your computer.
- **Call the right person for help:** Try not to panic if you are a victim. If you encounter illegal online content, such as child exploitation, or if you suspect a cybercrime, identity theft or a commercial scam, just like any other crime report this to your local police. There are many websites to get help on cybercrime. To name few
    - http://www.cybercrimehelpline.com
    - http://www.cyberpolicebangalore.nic.in,
    - http://www.cybercellmumbai.gov.in

3.4. STEPS TAKEN BY THE GOVERNMENT TO PREVENT CYBER CRIMES

The Information Technology Act, 2000 together with Indian Penal Code have adequate provisions to deal with prevailing Cyber Crimes. It provides punishment in the form of imprisonment ranging from two years to life imprisonment and fine / penalty depending on the type of Cyber Crime. However, the Government has taken following steps for prevention of Cyber Crimes:

- Cyber Crime Cells have been set up in States and Union Territories for reporting and investigation of Cyber Crime cases.
- Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.
- In collaboration with Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training.
- Programmes on Cyber Crime investigation. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cybercrimes for judicial officers.
- Training is imparted to Police Officers and Judicial officers in the Training Labs established by the Government.
- The Scheme for Universalization of Women Helpline has been approved to provide 24 hour emergency and non-emergency response to all women affected by violence.

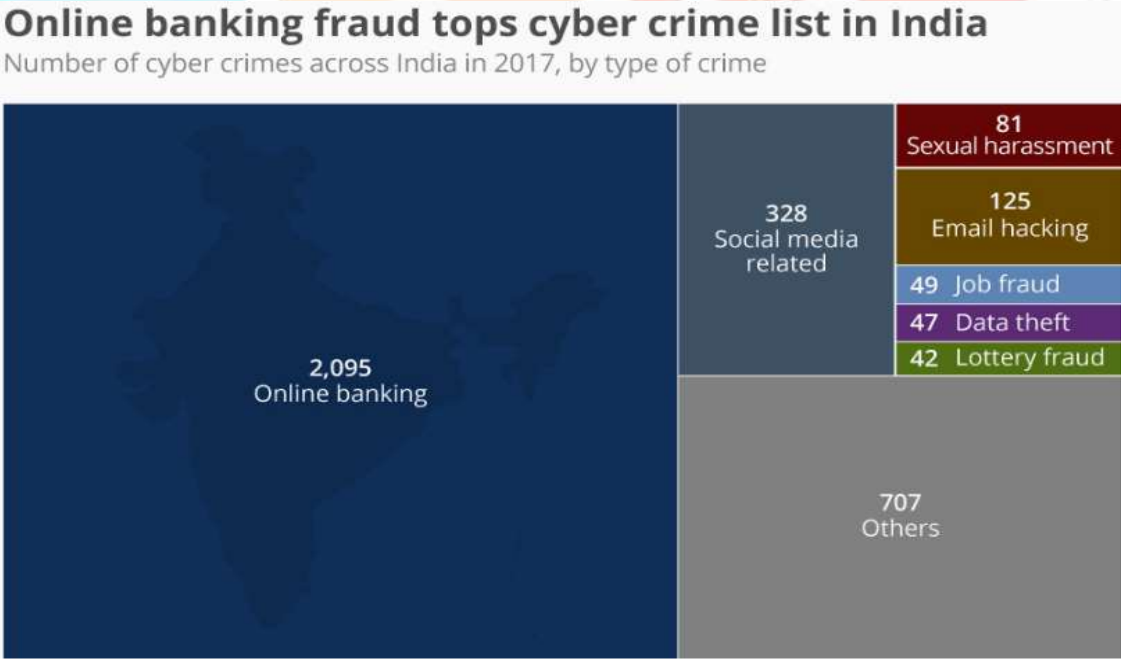
IV. METHODOLOGY:

4.1. Primary Data

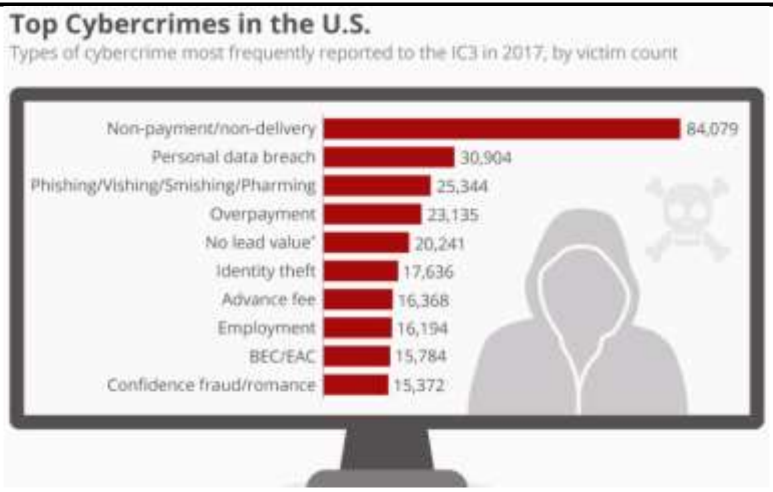
Primary data was not collected for the research paper.

4.2. Secondary Data

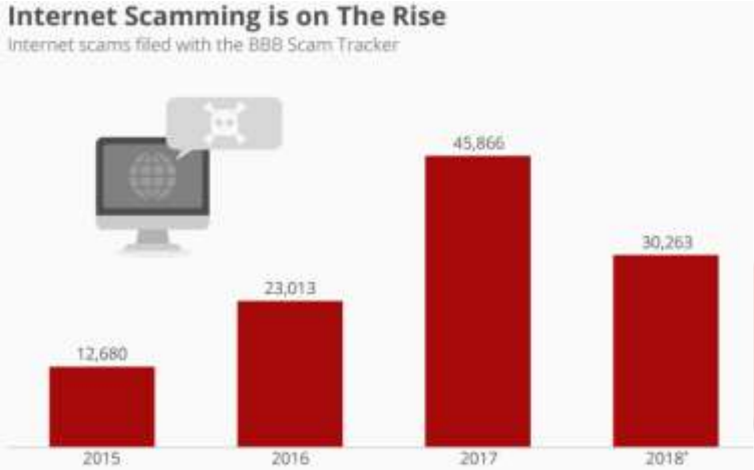
The secondary data has been collected. For this purpose various magazines and journals have been used as it is a conceptual paper. Thus, the focus is to know more about the concept, its application and the impact on economy via other parameters. Therefore qualitative and quantitative data have been used.



The number of cybercrime cases across India has risen drastically by more than 44 percent between 2013 and 2017 from about 2,400 to approximately 3,474. Police responsible for cybercrime in India blame the ease at which online information can be accessed as well as technological advancement for the drastic rise in the number of cases. Most of the cybercrimes across India are related to online banking. There were about 2,095 cases of online banking fraud reported in 2017. Due to the increasing number of cases, policy makers across the country have emphasized digital security as the key issue with regard to the government's push towards a cashless economy.



Cybercriminals are capitalizing on the massive amount of people who order things on the internet. According to the IC3, the Internet Crime Complaint Center, the top reported cybercrime in the U.S. was the non-payment or delivery of a good ordered over the internet. This type of cybercrime affected more than 84,000 people in 2017 alone. Trailing in a distance second are personal data breaches and phishing or pharming scams, both hovering just above and below 25,000 complaints respectively.



Internet fraud is responsible for more than $100 billion of private and company losses. Be it blackmailing state facilities or scamming someone with an alleged inheritance from a forgotten relative, the tactics of those scammers are pretty diverse. That means almost anyone can prove a target no matter if you are a digital native, a middle-aged corporate employee or a senior. As the Scam Tracker by the Better Business Bureau reports, internet fraud has skyrocketed in recent years with almost 46,000 filed scams in 2017 in the U.S. alone and already more than 30,000 by mid-August of this year.

V. CONCLUSION:

Cyber-crimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber-crimes can be committed single handed and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals.

REFERENCES:

1. https://krazytech.com /technical-papers/cyber-crime
2. http://pib.nic.in/newsite/PrintRelease.aspx?relid=132545
3. http://www.crossdomainsolutions.com/cyber-crime/
4. https://www.statista.com/chart
5. https://www.statista.com/chart/15069/number-of-internet-scams-in-the-us/
6. Jigar Shah (2016), Volume 01, Issue 01, PP. 11-16.
7. Kanika Chhabra and Gunjan Chhabra (2015), Volume 02, Issue 01, PP. 21-26.