RESEARCH PAPER

ON

INTERNET BECOMING NEW FRAUD HUB

BY

SATYA KARUNA

BBA LLB(H) 2nd YEAR

Abstract-

The Internet has proved as a boon for society, it's a place to get liberating experience but also there is the potential that society can be prone to cybercrime. The Internet is often described as a very useful tool, there is the potential for many of us to become victims to the growing pool of criminals who skillfully navigate the Net. Cyberspace often known as cyberweb is an environment that is intangible and dynamic. This paper present that Cyber Crime presents as new form of business for the Hi-tech Criminals.

This paper explores an overview of Cybercrimes, the cyber-crime perpetrators and their motivations. Different cybercrimes, and unique challenges and response issue which may be encountered during the prevention, detection and investigation are also been discussed in this research paper.

History of cybercrime-

Cybercrime didn't really find it footing until mid-20th century as digital revolution passed by the cyber criminals became early adopters of cybercrime. As the decade witnessed the creation of the first computer virus "the creeper virus", a self-replicating program invented by bob Thomas. This virus demonstrated how a software program could move across network. The first footmarks of [1]cybercrime could be seen in early 1830's when two thieves infiltrated the French telegraph system to gain access to financial markets, later in 1920th century after invention of telephone few teenage boys broke into graham bells telephone company and misdirected calls after which phone hacking became known. In 1940's Rene Carmilla a punch cart computer expert hacked into nazi data registry which further blocked the nazi's attempt to track and register Jewish people. In 1980's and 1990's when email became a popular communication form hackers started using email attachments for malware and phishing scams to spread computer viruses. Later in 2000s when social media networks gained popularity hackers started utilizing these platforms for data theft and cybercrimes.

Introduction-

A group of South Delhi teens create an Instagram group chat called [2]Bois Locker Rooms to share photos of women. Boys' locker room a well-known case related to an Instagram group

[1] Michael Aaron Dennis, Cybercrime, Britannica (Nov 3, 2023), https://www.britannica.com/topic/cybercrime.
[2] Amrtansh Arora, Bois Locker Room probe brings focus on rising crime on social media, INDIA TODAY (May 12, 2020 17:13 IST), https://www.indiatoday.in/india/story/bois-locker-room fake-profiles-crime-internet-teenagers-1677097-2020-05-12.

chat started by a group of school boys from Delhi, India in 2020. The group involves discussions objectifying women and use of graphic sexual language and also involved sharing of obscene pictures of females, mostly minor.

The Delhi commission for women takes Suo moto cognizance of case and it became first legal case to come out of Instagram chat in India. This was a prominent case of cyber bullying that involved nonconsensual intimate imagery. Cyber bullying in recent years has become relatively common and has contributed in many high-profile cases among which most of the victims end up choosing the path of suicide.

This research paper mainly aims to enlighten the society about cybercrimes which includes cyber bullying, cyber terrorism, financial fraud, sextortion, AI generated morphed photos and videos, etc. Cybercrimes are one of the most concerned topics now a days and half of them are UPI frauds (financial frauds). It is very different from any other crimes as it has no geographical boundaries so in most cases it remains unheard and unseen.

Main goal of our research paper is to range the knowledge of the crimes and violations that take place over the internet or cyber space alongside with the loss that are forced against offenders through this paper we are moreover trying to put emphasis on the security in cyber space. The growth and expansion of the developing technologies have started to run many cybercrimes in later 20th century. It has been a great threat to mankind since the ages.

Security against cybercrime is a coruscating part for social safety aspect of our country. The government of India has come up with it act 2000, IPC 1860, Indian evidence act 1872 and reserve bank of India act 1942. Any part of cyber space involving cybercrime are exceeding the boundaries of nation security involving both legal and technological aspects of complexities. The consistent efforts and cooperation of various nation are necessary to take action against cybercrime. The main tenacity of inscribing this paper is to range the content related to cybercrime amongst the communal people.

The internet is a very powerful tool and a very effective means of communication but is extremely vulnerable to cybercrime. To defend against cybercrime intrusion detection techniques should be implemented and administered. In order to get protected people need to follow preventive measures which negatively impact cyber-attacks. One of the many reasons of ongoing vulnerability is that we lack cohesive approach for defending our interest against cyber threats. We need to get unified in order to fight from these crimes as we are very clear with the fact that neither government nor the private sector can solve this problem by oneself.

Who are committing cybercrime-

1. Hackers- It is a term commonly applied to a person who intends to gain unauthorized access to a computer system. According to IT act 2000 sec 66 [3]hacker is a person whoever with the intent to cause or knowing that he is likely to cause wrong loss or damage to public or any person who destroys or deletes or alters any information residing in a computer resource diminishes its value or utility by any means is a hacker. A hacker can secretly control the victim's computer using it to commit crime or spread spam. His basic idea is to exploit the weaknesses in a computer system or network.
2. Crackers- They are the one who trespass computer software or security system with malevolent intent. It's the procedure of gaining unauthorized entry to systems or networks by breaching their security. Its similar as hacking but with illicit intent. Types of cracking involve- password cracking, software cracking, network cracking, application cracking, wireless cracking.

Why people commit cybercrime-

By the end of 2030 there will be more than 80 billion devices connected to the internet and every single device will be vulnerable to the hackers. We can expect this number to rise but what motivates hackers to hack? Why are hackers doing this? How do they find weaknesses to exploit?

1. Mostly for financial gain

   Attackers have several different methods including demanding some sort of ransom from the victim in exchange for breached data. Selling the information in dark wave or stealing money from victims via credit card or bank account.
2. Theft of intellectual property

   This is done either to gain some sort of market or military advantage. This type of attack is carried out via third party attackers so corporate or any government entity can deny of having any knowledge for the same.

[3] Hana Rhim, Differences Between Hackers and Crackers, Baeldung (September 13, 2023), https://www.baeldung.com/cs/hackers-black-white-gray-hat-crackers.

3. Revenge

   Revenge is a common motivation for hacking with financial benefit or disruption being a biproduct of their anger.

4. Fame

   Hackers claim responsibility for hacking high profile entity with an intention of gaining the recognition for their ingenuity and skills.

5. Recreational hacking

   They generally break into computer network for thrill to challenge themselves or for bragging rights in hacking community.

Types of cybercrime-

Internet is an indispensable tool for almost all type of cybercrime as more and more devices are enabled to communicate and connect themselves with the internet the hacker's strength is likely to multiply. The goal of the criminal is likely to steal information from, or cause damage to computer network. The perpetrators may be teenage students or may be professional of this field or may be terrorist. They use computer to commit a traditional crime. Example- child pornography where computer is used to produce possess or receive, distributed child porn so the computer may contain the evidence of crime.

[4]Types-

1. Crime against person
2. Crime against property
3. Crime against government

1. **<u>Crime against person</u>**

- **Cyberstalking**

[4] Nidhi Narnolia, Cyber Crime in India: An Overview, Legal Service India, https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html.

Cyberstalking is when a person is followed or pursued online in this privacy or personal life of a person invaded and their every move is watched. It is a form of harassment and can disrupt the life of the victim and leave them terrified. Staking or being followed may include monetary identity theft, vandalism, solicitation for sex or doxing and blackmailing. Cyberstalking is often accompanied by real time or offline stalking. Stalker may be an online stranger or a person whom victim knows very closely. [5]Cyberstalking is a criminal offence punishable under sec 67 of information technology act 2000. A conviction can result into a restraining order, probation or criminal penalties against the assailant. The main target of cyberstalks are mostly females, children, emotionally weak or unstable people.

Online anonymity makes it challenging to trace cyber stalker but still we can contact the appropriate authorities after collecting the evidence of their actions. Second step is notifying local police having an official complaint if the behavior persists or escalates. Third step is reporting them to the sites or services they have used.

- Types of cyberstalking-
    - Webcam hijacking- internet stalkers attempt to trick the victim into downloading an putting a malware infected file on their device that may grant them access to your webcam. This is a devious method that probably won't let the person suspect anything strange.
    - Catfishing- it happens via social media sights for example Facebook, Instagram. Herein internet stalkers may counterfeit user profiles to approach victims as a companion of a companion with the intention of stalking or hacking.
    - Installing stalker ware- it is a kind of software or spyware which keeps track of the location or enable the access to text and browsing history, make an audio recording, etc. the important thing to note is that the software runs in the background without the knowledge of the victim.

[5] Lauren Mak, what is Cyberstalking? How to Recognize It and Protect Yourself Lauren Mak, vpnoverview (oct 02, 2023), https://vpnoverview.com/internet-safety/cybercrime/what-is-cyberstalking/.

- Protective measures-
    - Logout all the social networking sites of your devices when not in use
    - Set strong and distinctive password for your online accounts
    - Make use of privacy settings provided by social media sites and make all the information restrictive to nearest of friends
    - Remove any future events you are close to attend from social media sites
    - Avoid sending personal emails or sharing sensitive information when connected to unsecured public Wi-Fi

- **Financial crime**

[6]Financial fraud includes cheating, credit card frauds, bank robbery, UPI frauds, money laundering, etc. In a recent fraud case, a website offered to sell alphonso mangoes at a throw away price distrusting such a transaction very few people responded to it and supplied the website with their credit card numbers, these people who ordered through this website were actually sent mangoes now the website-built trust among the people. Now thousands of people from all over the country responded and ordered mangoes by providing their credit card numbers, the owner of the website was later proven to be fraud and he flew away taking numerous credit card numbers which resulted in huge loss to card owners. This was a very common example of [7]financial cybercrime which is basically an act of obtaining financial gain through a criminal activity such as stealing or gaining access to financial account in order to initiate unauthorized transaction. The consequences may involve loss of large sums that can impact the whole economy of a company or community that can even lead to bankruptcy in several cases where company is small. Reputational damage in eyes of stake

[6] Prateek Kothari, The Impact of Cybercrime on the Indian Economy and Society, Legal Service India, https://www.legalserviceindia.com/legal/article-11766-the-impact-of-cybercrime-on-the-indian-economy-and-society.html.

[7] Prateek Kothari, The Impact of Cybercrime on the Indian Economy and Society, Legal Service India, https://www.legalserviceindia.com/legal/article-11766-the-impact-of-cybercrime-on-the-indian-economy-and-society.html.

holders and clients when it comes to private individual, they may experience having their account emptied, savings stolen or debts taken up in their name.

- Prevention of financial fraud-
  - Always be alert and careful when shopping online or making online transaction or signing into your online bank and government portals.
  - Always make payment or transfers through official sights. Avoid using public WIFI during making payment or inputting any OTP.
  - Be careful not to click on any suspicious link, always verify senders' identity.

- Types of financial fraud-
  - **UPI fraud**

    This happens when fraudsters ascend fake UPI links or ask for sensitive information such as UPI pins, passwords or OTPs through text messages or phone calls. Once these fraudsters receive information, they use it to transfer funds, or make purchases without user's consent.
  - **Credit card fraud**

    It happens when a criminal steals someone else credit card information and uses it for their own financial gain. It is basically unauthorize uses of [8]credit card to make unauthorize purchases or withdraw cash. There are two types of credit card fraud

    i. Application fraud

       When a fraudster uses illegally obtained credit card information to open a new account in victim's name.

    ii. Account takeover fraud

[8] Nidhi Bajaj, Financial frauds in India: all you need to know, iPLEADERS (March 10, 2022), https://blog.ipleaders.in/financial-frauds-in-india-all-you-need-to-know/.

When a criminal uses victims personal identity information to take control of their account and misappropriate funds.

- **Money laundering**

The illegal process of making large amounts of money generated by criminal activities and converting it into a legitimate source. money laundering involves a complex process of cleaning "dirty" funds to rate the appearance of legality so that criminal can spend money without arousing suspicion. This type of money is obtained by drug trafficking, corruption, embezzlement or gambling.

Stages of money laundering-

i. Placement

Dirty cash is introduced into financial system

ii. Layering

Criminals try to distance the money from the crime source and mostly deposited in banks.

iii. Integration

Money reenters the economy through clean investments and money is invested in purchase of luxury assets, financial investment, industrial investments, etc.

- **Child pornography**

[9]Child pornography refers to any content that depicts sexually explicit activities involving a child. Downloading, exchanging, and producing any audio-visual material that includes any such material where in a minor is [10]sexually abused is a criminal behavior which can be of great academic and social concern.

In a recent incident a student of Airforce Bal Bharti school, Delhi was teased by all his classmates for having thick lips, tired of those jokes he decided to

[9] Suzanne Ost, Child Pornography and Sexual Grooming Legal and Societal Responses Cambridge University Press (May 2010), https://www.cambridge.org/core/books/child-pornography-and-sexual-grooming/62B5B2BE421B4A9A85C35C603E5015B0.

[10] Sarah Sheppard, Understanding Rape and Sexual Assault, verywell mind (January 04, 2023), https://www.verywellmind.com/what-is-sexual-assault-4844451.

get back and revenge his classmates. He scanned photographs of his classmates and teachers and morphed them with nude photographs and put them on a porn website. Father of one of the class girls when saw his daughter on the website, lodge a complaint in nearest police station, action was taken to remove all the pictures and the student was sent to correction home.

In another incident which took place in Mumbai, a Swiss couple forced alum children to appear for nude photographs and child porn. Minor girls were forced for sex videos with minor boys and later these videos and photos were posted on websites which were specially designed for pedophiles. The Mumbai police arrested the couple for child pornography.

Child pornography includes sexual intercourse, sodomy, fellatio, masturbation, sadomasochistic abuse, bestiality and sexually alluring displace of genital or public area. Production, distribution and possession of child pornographic material is prohibited under sec 14 of [11]POCSO ACT 2012 and the punishment include 5 years of jail with or without fine.

- Victims of child pornography-

  They are basically minors under 18 years old. They mostly know the pornographers and their actions are coerced through grooming and other pressure. They can also be abducted or physically forced. The viewers of child pornography are mostly college students introverted in nature, not have a criminal record and socially active people. They are mostly involved in victim blaming. They basically blame society for their actions. [12]Victimization never ends.

- Impact on the victims-
  - Physical injury and Pain included sexual transmitted diseases
  - Frequent headaches and stomach ache
  - Ongoing feeling of humiliation and lack of privacy
  - Pain in sexual organ, distorted and unhealthy sexuality
  - Anxiety, Depression, PTSD

[11] Ritika Sharma, POCSO Act: everything you need to know, iPLEADERS (May 13, 2022), https://blog.ipleaders.in/pocso-act-everything-you-need-to-know/.
[12] Abby Conklin, what is Victimization? study.com (July 22, 2022), https://study.com/learn/lesson/victimization-overview-types-effects.html.

- Impact on society-
    - Fuels the demand of child pornography
    - Existing child pornography may normalize sexual activities among children and may increase the chances of a minor being a rapist or create new child pornography.
    - Existence of child pornography may increase sexting among children and may indulge into sexual behavior.

- **Revenge porn and blackmailing-**

  It refers to publication of obscene photos and videos visualizing sexual organs on the internet without the consent of subjects of the images or videos. [13]The victims are primarily young women. In recent years there has been noticed the increase in activity of revenge porn majorly due to sexting. Sexting means sending of sexually explicit, personal messages and images. Sextortion or webcam blackmail happens when intimate images and videos are recorded without consent of subject and use for financial and sexual exploitation of the person. The majority cases involve coming in a relationship with the victim where the blackmailer assumes identity of a well-maintained man who after gaining the victims trust will quickly persuade them into sending intimate images or videos or will record sexual activities which later will use for blackmailing them for further sexual content. Victims facing the conundrum generally end up taking disastrous steps like suicide or being a criminal themselves which is an outcome of criminal behavior burgeoning revenge.

- How to protect yourself-
    - Avoid sharing any compromising photos
    - Don't keep compromising photos of others on your device
    - It is important to have effective communication between parent and children in order to prevent problems and resolve them.

[13] Rohan Kumar, Privacy in Internet era, Private data and Blackmailing Revenge Porn, Legal Vidhiya (April 6, 2023), https://legalvidhiya.com/privacy-in-internet-era-private-data-and-blackmailing-revenge-porn/.

- If you discover your compromising images on any site, directly contact the administrator and demand for their immediate withdrawal.

- **AI morphed photos and videos-**

Cyber criminals find images of victims on social media and then edit them using AI to make them look realistic and sexually explicit. The photos are sent to victims for [14]sextortion or harassment, once circulated victims can face significant challenge in preventing the continual sharing of the manipulated content or removal from the internet. Those whom suspect that they are victim of AI morphed videos and photos can contact the FBIs internet crime complaint center.

Deepfake videos and photos are one of the examples where we use AI to replace a person's appearance or voice with another's, making it seem like as if they have done or said things which they haven't.

- Legal remedies of AI morphed photos and videos-
  - If deepfake videos are spread without the consent the victim the victim can potentially file the complaint under sec 66 of IT act that deals with punishment for cheating by a person using a computer resource. Under this provision accused may be imprisoned for 3 years and a fine up to 1 lakh.
  - Rule 3(2)(b) states that within 24 hours of filing such complaint the authorities shall take measures to disable or remove the access of such content
  - IPC sec 499 and sec 500 states that if a video is created for harming the reputation of the individual then he can file a defamation suit against the creator.

- **E-Mail spoofing and SMS spoofing-**

[14] Himel Mondal, Characteristics of Cyber Sextortion in India: Content Analysis of Online Newspapers, https://www.researchgate.net/publication/361614520_Characteristics_of_Cyber_Sextortion_in_India_Content_Analysis_of_Online_Newspapers.

A [15]spoofed email that appears to originate from one source but actually has been sent from another source. Example- A has an enemy B who spoofed her email and sends obscene messages to all her colleges since the email appears to be originated from A, her friends could take offence and relationships could be spoiled for life. This could have ruined A's image among her college and could have costed her, her job. Email spoofing can also cause monetary damage. In a recent case a teenager name Divya Sonali from Gurugram made millions of dollars by spreading false information about certain company's merger whose shares had been sold on a really less price. This misinformation was spread by sending spoofed emails porously from news agency like India today and zee news, to share investors and brokers, who were informed that the companies were doing really badly the cost of shares had been declining even after the truth came out the values of shares did not go back to the earlier level and the company's and shareholders lost a lot of money.

- How to identify spoofing email-
    - Check to see if email address appears from a legitimate source and the name and other details match up
    - An email address that doesn't match the senders display name and specially if the domain of the email address looks suspicious that's a sign of email spoofing
    - Spoofing email often contain messages to provoke essence of emergency to scare or alarm you
    - Spoofing email generally request for personal information to mix you up in phishing scam
    - Avoid clicking links or downloading attachments that appears to be suspicious and look for the text used in the email, whether or not reported already on internet
    - Look for inconsistencies in email signature such as telephone numbers and other personal details

[15] Crissy Joshua, SMS spoofing: An overview + 5 SMS spoofing types to avoid, Norton (June 28, 2023), https://us.norton.com/blog/mobile/sms-spoofing.

- When in doubt avoid opening any unknown or suspicious email

- **Cyber Defamation-**

It is a publication of a false or wrong statement about an individual or person in cyber space world that can damage their reputation. It is also known as online defamation and can occur over digital communication channel such as social media platforms, emails or instant messaging. It is communication of false statement that can take many forms including malicious gossip, false accusation, or untrue statement. It can be intentional or unintentional, can involve both individuals or organizations.

- Why [16]cyber defamation is a big issue-

It can have significant and lasting impact on a person's reputation, personal and professional; life and even their mental health. Individual who is engaged in cyber defamation will subject to civil and criminal penalties. Through social media, internet defamation has been raised as a concern because it's very easy to publish and share fake information.

To prove defamation following elements must be generally established-

- The statement was false or must be factually inaccurate
- The statement was communicated to a third party or must be communicated to at least one other person in writing or verbally
- The person or organization has been suffered from loss of reputation and the statement must have been made with malicious intent or with reckless disregard
- The statement has been costed to loss of business or damage to personal relationship or emotional distress.

- Laws regarding cyber defamation in India-

[16] Anshika Gubrele, Defamation in the Internet Age: Laws and Issues in India, iPLEADERS (June 1, 2019), https://blog.ipleaders.in/cyber-defamation-india-issues/.

- Sec 499 of IPC- if a person attempts to slander somebody to bring down its standing who ought to have criminal aim to defame anybody with such information.
- Sec500 of IPC- the person under sec 499 if found defaming someone can be punished with fine and two years of prison
- Sec 469 of IPC- if a person makes such a phone call with an intention of hurting g an individual, it is an offence culpable of three years of prison and fine.
- Sec 503 of IPC- if a person suffers any kind of injury to himself or his property then the accused can be charged for three years of prison or fine or both
- Sec 65A and 65B of evidence act- any electronic record printed on paper or media will be accepted as evidence as cyber defamation.

- **Carding-**

It is a type of cyber-attack which involves stealing a person's credit card details for buying large stuff from that card from ecommerce site and then using or selling it at lesser rate. [17]Carding lures victims through these hackers by randomly texting the victims and asking them their personal details for updating system. The cybercriminal frequently deploys bots to steal credit card information attempting to figure out which card will pass the verification process during the large-scale purchase. Sometimes the cyber criminals take the credit card information from the dark web and use card on various ecommerce website to buy expensive items without the owner's consent by using OTP bypass mechanisms.

- How does the carting technique work-
  - Carting typically starts with a hacker gaining access to a stores credit card system and to grasp numerous credit card numbers

[17] James Chen, What Is Carding? How It Works, Prevention Methods, and Examples, Investopedia (March 14, 2022), https://www.investopedia.com/terms/c/carding.asp.

- Hackers might exploit the weaknesses in security software systems and technology intended to protect credit card account
- The hacker then sells the list of credit card or debit card numbers to a third party we call as carder who uses the credit card information to purchase stuff
- After thousands of attempts on various ecommerce platforms and websites, the card that successfully works get listed for the sale

- Ways for cybercriminals to steal the credit card information-
  - The carders can obtain credit card details from [18]dark web since it is uncensored and anonymous
  - Phishing websites where they mask themselves as bank representator
  - Tricking the users to install such applications which steal their financial
  - Implementing credit card skimmers on front of sale machine and ATM
- How to detect carding fraud-
  - Abnormal notifications over emails and notifications over email and SMS
  - Increased failed attempt of payment
  - Reputative views of payment steps on ecommerce sites

- How companies prevent carding fraud
  - Address verification system- It compares the billing address supplied at check out in an online purchase to address of record at credit card company
  - Card verification value (CVV)- CVV is a three- or four-digit number that adds an extra layer of security when a person is

[18] Andrew Bloomenthal, What Is the Dark Web and Should You Access It, Investopedia (June 06, 2022), https://www.investopedia.com/terms/d/dark-web.asp.

not around. The issuer can approve or decline the transaction if CVV verification fails

- Multi factor authentication- It is a security technology that requires more than one method of authentication to verify users' transaction
- Captcha- (Completely automated public turning test to tell computers and humans apart) "it is a security measure that protects users from password decryption by asking the user to complete a test that proves that it's not a computer attempting to break into the account
- Velocity check- It keeps a check of the number of attempts, the card is used in a limited time period. Typically, users do not make multiple payments in a quick succession, especially beyond the capacity of a human being

- Punishments of carding-

According to sec 66(c) of information technology act 2000 any person who is frequently caught committing carding shall be punished for imprisonment which can be extend up to three years or fine may up to rupees ten lakhs.

2. **Crime against property-**

Now a days people rely more on machines than on themselves, the manual record that needs to be save and safeguarded are made available when needed through the computer databases. Through the development of new networking and communication technologies also come new ways to abuse them. The manual records are in potential danger when uploaded on computer databases. They are prone to any mis happenings that could turn into a major catastrophe. In cybercrime against property the hackers utilize software to access the sensitive data to steal the information involving intellectual property such as patent, trademarks, copyrights, etc. cybercrime against property comes in different forms such as-

- **Cybersquatting or Domain squatting-**

It's the abusive practice of registering and using an identical internet domain which is similar to another trademark, service marks, company names or

personal names with the bad faith or bad intention of hijacking any domain for personal and financial profits or for delivering any such payloads which include computer viruses or with an intention of stealing intellectual property. Cybersquatting involves deliberate registration of domain name in violation of trademark rights. It also includes warehousing which is the practice of registering a collection of domain names corresponding to trademark with intention of selling the registrations to the owners of trademarks within the notion of cybersquatting

- Types of cybersquatting-
  - Identity theft – This involves an attacker masking the online persona of a legitimate business by registering a domain that looks identical to the domain of the victim. Users trying to reach the companies site can accidently access the phishing domain. It also occurs when a hacker requires a previously registered domain whose owner has not registered on time in such case the owner of the domain needs to pursue legal action in order to recover the domain
  - Typo[19] squatting-

    It involves the registration of domain name that are misspelled versions of popular brands or websites. It can be done by-
    - dropping a dot after www
    - dropping by letter
    - switching two letters
    - pressing a wrong key
    - using similar looking character
    - doubling character

    the website address be look very similar to the legitimate one with just one latter change or a hyphen added. The web squatter gets its working because they capitalize when people make error.

[19] Elizabeth Quinn, How to Do the Squat Proper Form, Variations, and Common Mistakes, verywell fit (July 25, 2019), https://www.verywellfit.com/.

- Reverse [20]cybersquatting-

  This occurs when a hacker uses the rules as they urgently stand to their advantage. The online predator begins by picking an established website as a victim. The next step is to incorporate under the same name. once everything is in place, they will play the victim card that the genuine owner is web squatting utilizing the institution that they own and attempt to take possession of that website by using question of law

- Name jacking-

  One of the most shred FORMS is name jacking which occurs when a squatter creates a false website using the real name of the famous person. This situation frequently occurs in domain or social media profiles are registered in the name of celebrities by cyber squatters. It may not always be possible to prove that name jacking was on purpose thus making the prosecution of crime more challenging.

In India, victims of cybersquatting can deal with it through the following ways:

1. They can send cease-and-desist letters to the cybersquatted.
2. They can opt for arbitration under [21]ICANN's rules,
3. Victims of cybersquatting can go for a trial to a state or federal court.

SOME INDIAN CYBER-SQUATTING CASES

Yahoo! Inc. v. Akash Arora

It is the first case that was reported in India regarding cybersquatting. In this case, plaintiff was a registered owner of the domain name "yahoo.com". He obtained an interim order which restrained the

[20] Jordan Smith, How to Do a Squat Correctly, Plus the Best Variations to Spice It Up, RUNNER'S WORLS (MAR 15, 2023), https://www.runnersworld.com/training/a32256640/how-to-do-a-squat/.
[21] Peter Lohsin, ICANN (Internet Corporation for Assigned Names and Numbers), Whatls.com (17 April 2018), techtarget.com.

defendants from dealing the name "yahooindia.com" or any other trademark similar to the trademark of the plaintiff.

In the well-known case of Marks and Spencer's, the defendant registered enlisted trademark of mark and Spencer's as "www.marks and spencer's .com" with the mala fide aim to offer it at a higher cost to the legitimate proprietor. In the judgment of "One in a million case" the English court conceded injunction against cybersquatting of domain name Marks and Spencer, the offense of cybersquatting additionally involves unjustifiable competition where a defendant deliberately takes uncalled for favorable position of a well-known trademark.

Legal Remedies:

According to Section 135 of the Trade mark Act, 1999 legal remedies for infringing registered trademarks or the passing of injunction, damages or account of profits or delivery of goods or destruction of infringing goods.

Section 103 provides penalty for the applying of false trademarks i.e., punishable with infringement of not less than 6 months and may extend up to 3 years followed by fine not less than Rs. 50000 extended up to 2 lacs.

If a mark is registered the common law remedy of passing off is available to the owner but in case in which his mark is registered, he also possesses the statutory right to file the action for infringement under Trademarks Act 1999.

- **Cyber vandalism-**

It is a malicious destruction of digital property. It usually targets websites and other technical products and also be used in threaten individuals or institutions. Cyber vandal uses all sort of tools to deface website and delete files, takeover users account or send spam and viruses. Whereas traditional ways of vandalism mainly include the vandals leaving his/her mark for

everyone to see. [22]Cyber vandalism gives the perpetrator virtual anonymity by allowing them to commit their crime from anywhere anytime by being anonymous.

Types –

- Disruptive cyber vandalism-

  This involves deliberately introducing bugs and viruses into programs to disrupt the files completely and can lead to everything from data loss to complete wiping up of source code of program

- Destructive cyber vandalism-

  This type of vandalism includes destructive cyberattack without any obvious profit and motive.

- Defamatory cyber vandalism-

  This include false and damaging statement made about a person or entity on the internet by hiding the identity and being anonymous.

Common forms of cyber vandalism-

- Website defacement –

  It involves full change in content and visual appearance of an existing website without knowledge of the owner. It involves altering the website with the hateful messages to harm the reputation of the owner such modifications are achieved by targeting weakness of the website. The main target of website defacement are large corporations, political figures, religious and government sites.

- Software sabotage-

  This generally results in destruction or damage of computer hardware. Sabotage may require some sophistication of computer assisted security system are manipulated=d to do harm to itself. This involves theft of services, theft of property and financial crime. It can also involve the intentional distributed or stolen software which can be unknowingly installed and be openly used which can lead to public exploitation and can cause immense damage.

[22] Jeremy Wanamaker, What Is Cyber Vandalism and How Can You Prevent It, Complete Network (Jul 28, 2023), https://complete.network/what-is-cyber-vandalism/.

- Account hijacking-

  It includes taking over a user's account on an application to access their information, published content in their name to commit fraud or implant malware or post obscene content. Account hijackers exploit weaknesses by use of weak password or improper security of websites. It is a type of identity theft which hackers generally use to perform financial transactions, create new accounts or carry out some illegitimate activities.

- DNS cache poisoning (domain name system cache poisoning)

  It is also called [23]DNS spoofing. It is an act of placing false information in DNS resolver in order to get a wrong entry or IP address of the requested site from the DNS server. In DNS spoofing the attacker is able to inject his own entry into local DNS server ion order to look exactly like the legitimate server.

  Laws regarding cyber vandalism-

  Under IT act 2000 the remedy provided under cyber vandalism is in form of monetary damage or compensation which should not exceed more than one crore

- **Cyber trespass-**

  It is computer crime which involves unlawful access to computers without proper authorizations for gaining financial information. A person can be said to be guilty of cyber trespass if he intentionally or without proper authorization tries to access, alter or delete any such information in computer system or network then it is called as cyber trespass. The key element for the offence of cyber trespass is lack of authorization to access a computer system. In case of trespass where just cracking is involved it is of civil nature but once the intention of causing harm or damaging the system involves it becomes of criminal nature. The computer may be used as a tool

[23] Jeff Thompson, How to Prevent DNS Poisoning and DNS Spoofing, AT&T (April 17, 2020), https://cybersecurity.att.com/blogs/security-essentials/dns-poisoning.

for breaching of right, [24]computer theft, invasion of privacy, forgery or password disclosure.

Legal remedies-

A person involved in theft, trespass, forgery, invasion of privacy may be imprisoned with 3 years or fine not exceeding 50 thousand.

A person involved in computer password disclosure may be imprisoned for 1 year and fine not exceedingly more than 25 thousand.

A person accused of removing or deleting any data either temporarily or permanently may be imprisoned for 6 years and fine not exceedingly more than 1 lakhs.

- **Intellectual property crime-**

  It is committed when someone sells or distributes counterfeit or pirated goods such as patents, trademarks, industrial designs or literary and artistic work for industrial gain. The resulting adverse social and economic effects include loss of jobs and livelihoods.

  - [25]Counterfeiting is done in industrial property. It is the manufacture, importation and distribution or sale of goods which falsely carry the trademark of a genuine brand without permission or for gain or loss to another.
  - Piracy is done in copyright material. It is an unauthorized copying or production, use, distribution of materials which are protected by intellectual property rights. Copyright includes literary and artistic works, music, dance, tv shows, radio shows, etc.

    Laws enacted to protect IPR-

  - The patents act 1999-

    It offers exclusive marketing rights for the time span OF 5 YRS
  - The trademark bill1999
  - Copyright amendment act 1999
  - Geographical indication of goods registration and protection bill 1999
  - Industrial design bill 1999
  - Patent bill 1999

[24] Ananya Talpare, Computer Theft - Protecting Data and Identity, Allied universal (13 March 2014), https://experianverify.com/

[25] Karnika Seth, what is Computer Forgery and Counterfeiting, karnikaseth.com (12 March 2013), https://www.karnikaseth.com/what-is-computer-forgery-and-counterfeiting.html.

- Remedies include
  - Copyright infringement

Copyright protection is given to the owner of any published, artistic, literary, scientific work. When these proprietary creations are utilized by anyone without the permission of owner it leads to copyright infringement. For example- if A wrote a book and uploaded it on a website and sold on internet and if a printing press company B sold its hardcopy without permission of owner or even copying half the content from the source then it will lead to [26]copyright infringement.

- Linking-

When a person knowingly links to works that clearly infringe somebody's copyright, like pirated music files or video clips of commercially distributed movies and music videos. In this situation, one might be liable for what is known as "contributory copyright infringement." It occurs by intentionally inducing or encouraging direct infringement of a copyrighted work. As long as a person do not know that a work infringes someone's copyright, he can't be held liable for contributory infringement for directing users to that work. On the other hand, it is not necessarily safe to simply claim that one "didn't know" when the circumstances make it clear the material you link to is infringing. Consider removing embedded videos once you've been notified by a copyright owner that they are infringing.

- Framing-

When a website frames something it makes the contents of another website viewable from its own site. It may lead to legal issues involving copyright and trademark laws because the website arguably alters the appearance of the framed website also the framing website may give the impression that the site being framed endorses or is related to the offending site.

- Inlining-

It allows a special type of link to be inserted into the webpage that allows viewers of that page to see the graphic file through the link on a separate webpage. A federal appeals court found that this practice amounted to copyright infringement.

[26] Triveni Singal, Concept of contributory copyright infringement claim with special emphasis on the recent case of Harold Davis vs. Pinterest, ipleaders (12 September 2021), blog.ipleaders.in

3. Cybercrimes against government-

It refers to any illegal activity that is aimed at a government agency or entity using computers or any online platform or other forms of digital technology. Such crimes can be committed by individuals or groups and they can take many forms.

- **Cyber terrorism-**

  It is a politically motivated attack against the information system programs and data that threaten violence or results in violence. It includes any cyberattack that generates fear in the population. It often results to physical harm. The attacks that are intended to be disruptive or have a political agenda can qualify as cyber terrorism.

- Methods used for cyber terrorism-
  - Advance persistent threat-

    It uses sophisticated methods to gain network access, once they get the access, they stay undetected for a period of time with intention of stealing data. Organizations like defense, manufacturing and financial industry are common target of [27]APT attacks.

  - Computer viruses-

    Malware target the IT control system like transport systems, power grid, military system, etc. are common target of computer viruses.

  - Hacking or cracking-

    It is done to gain unauthorized access to steal critical data from different institutions or government offices and large businesses.

  - phishing-

    phishing attacks are basically done to steal victims' identity. The attacker attempts top collects the information through the targets email and using that email the attacker tries to access the victim system.

  - ransomware-

    it is a type of malware that steals the data and holds its information system hostage until the victim pays the ransom amount.

[27] Eriz Hasson, Advanced persistent threat (APT), Imperva (Nov 08, 2023), www.imperva.com.

Examples of cyber terrorisms-

- They mostly aim to spy on rival nations and gather intelligence such as troop location or military strategy. These acts are mostly sponsored by government.
- Attackers often aims to get unauthorized access of communication channel that control military and other critical technology.
- cyber terrorist also targets public necessities like water treatment plant that might cause a outrage or disrupt a pipeline or oil refinery which can cause a massive panic and fatalities.

- How to defend against cyber terrorisms
  - Use strong password
  - Follow cyber security news and government warnings
  - Create a culture of cyber awareness and look out for anything suspicious
  - Businesses should demand transparency from all members regarding cyber security practices
  - If cyber threat is received by a telephone, then record as many details as possible and contact terrorist hotline number
  - Set up a two-factor authentication factor against hacking

- **Cyber warfare-**

It is usually defined as cyber-attack to target a country and its min motive is to destruct civilian infrastructure and disrupt critical systems, create havoc on government resulting in damage to the state and even loss of life. In most of the cases these most attacks are carried out by terrorist organizations seeking the goal of a hostile nation. The cyber warfare attacks include-

- [28]Espionage-

It is basically done to steal the secrets and monitoring the movements of other country. These can be done through spear phishing and botnets to compromise sensitive computer system information.

- Sabotage-

The government organizations give leverage on insider threats such as dissatisfied or careless employees. The such hostile government may steal information, destroy it. It can be used for a simple disturbance of government service or also to generate panic to demand for extortion and

[28] George Elise, Espionage to Cyber Espionage, Cyber espionage channel (14 January 2016), george.lekatis@cyber-risk-gmbh.com

spying by enemy government. The majority attacks target essential in fracture such as finance, defense and industry. Oil and nature gas plant are most prone to these kinds of attacks.

- Denial of service (DoS)attacks –

[29]DoS attacks prevents the users by accessing a website by flooding it with fake request thus forcing the website to handle these requests. This type of attacks disrupts the critical oppositions and systems and they block access to the sensitive websites.

- Economic disruption-

In economic disruption the attackers targeting computer networks that have already established economically such as stock market, payment system, they also target banks to steal money and block people from accessing funds.

- Propaganda attacks-

This is mainly done in an attempt to control the mind of people living in a target country. It can be used to expose embarrassing truths or create a fake situation to make people lose trust in their government and country or make the citizens of the target country on the side of enemies.

- **Software piracy-**

Software piracy is an act of illegally using copying, modifying, distributing or sharing computer software protected by copyright laws. A software pirate is a person who intentionally or unintentionally commits these illegal acts. Copyright laws have been created to make sure the developers receive an appropriate credit and compensation for their work. Whenever software is used copied or sold illegally, the copyright holders lose their recognition and payments which would be coming from their piece of work. The most common license [30](EULA) and user license agreement is used foe software protection. It is a legal contract between end user and software manufacturer which include different clauses top forbit the user to share the software with others.

- Types of software piracy-
  - Soft lifting or end-user piracy-

When a person purchases a piece of software and share it with people who are not authorized to use it then it is soft lifting and end-user piracy. This often happens in educational or corporate environment where the user only pays licensing fees for one software program but downloads it on multiple computers.

[29] Rutika Shahi, what is a denial-of-service attack (DoS), Paloalto networks (12 April 2019), http://Paloaltonetworks.com.

[30] Ruchir Drake, what is an end-user license agreement (EULA), Ironclad (Dec 23, 2016), https://ironcladapp.com.

- Counterfeiting-

It is the illegal copying, distribution or selling of licensed computer software. Other element that comes with software may also be counterfeited. For example, security feature, packaging, registration information, license agreement. Cyber criminals usually steal counterfeit software to sell it to a lower price than the original.

- Hard-disk loading-

The computer seller buys a legal piece of computer software, copies it, installs it on a computer's hard disk and sells the computer. This form of commercial software piracy is called hard- disk loading. Having software already installed makes the computer more attractive for buyers. Most of the buyers are unaware of purchasing unlicensed software.

- Client-served overuse-

When number of users using a particular software are allowed by the company to exceed the number of licenses the company have for software then the situation is called client-server overuse. This happens when the company installs the software on its local area network instead of an individual computer making it possible for the multiple users to use the same software at the same time.

- Online piracy-

It is illegals selling, acquiring or sharing of software on the internet. It is committed on the sites that sell counterfeit, outdated or pirated software through am online auction. It can be done through websites that offer to download pirated software program for free or the website that allows to exchange pirated software.

- Risk of using pirated software -
  - Pirated software may be cheaper but one will have to face increased risk of unlicensed software malfunctioning or crashing.
  - As an unauthorized user the user won't receive any update or customer support from the software manufacturer.
  - One will have to put their online security at risk because illegal and counterfeit software might infect your device with virus's malware or adware.
  - The user might have to face legal consequences and financial penalties due to copyright violation.
- How to protect yourself from software piracy-
  - Buying software program from authorized manufacturers and dealers.
  - Visit the official site instead of near identical site set up by the cyber criminals when downloading any software from the publisher's website.

- Scan the files for the viruses, there is always an chance that one might open an attachment in a random email and unleash enemy virus or malware.

Examples-

- Downloading copyright movies, games, songs, apps, etc. from shady websites in order to get it free.
- Streaming unauthorized content
- Buying a PC with unlicensed software installed in it.
- Purchasing a single user license and using it on multiple devices in order to save cost.

- **Possession of unauthorized information-**

  A person is said to commit an offence of possessing and unauthorized confidential personal information in any form may be email or physical documents identification card or information stored in any digital form. The person who has possessed any confidential personal information of any another person can defend himself that he did so that the possession was authorized by law and was by the consent of another person to possess the confidential personal information.

How to file a cybercrime complaint-

It can be filed online on the nation cybercrime [31]reporting portal. The rapid advancement of technology has made cyber criminals coming up with new ways to exploit the victims. From hacking the personal information to financial frauds, the cyber criminals are continuing to evolve. Nation cybercrime reporting portal is an initiative of government of India to facilitate victims reporting cybercrime online. This portal is exclusively created for cybercrime complaints which specially focuses on women and Childrens. Complaint reported on this portal are dealt by police based on information provided. 1930 is national cybercrime helpline number. One can file complaint by calling on this number by providing necessary details such as name, account number, mobile number along with the accurate details of your complaint. The complaint can be filed anonymously too. You can also track the status of your complaint. In case of anonymous complaint, you do not need to provide any personal information.

[31] Swati Shalini, what is Cyber Crime in India & How to File Cyber Crime Complaints, myadvo, https://www.myadvo.in/blog/how-to-file-a-cyber-crime-complaint-with-cyber-cell-in-india/.

However, the information related to the complaint should be complete and accurate in order for the police to take necessary action. You will need to register yourself on this website using your phoner number and you will receive an OTP on your number which will be valid for 30 minutes. Once you successfully register yourself on the portal you will be able to report the complaint.

Conclusion-

Cybercrime is inflicting havoc on the global economy and national security. It also lay down a negative impact on social stability and day to day individual life. Criminal behavior on the online platform or cybercrime, presents as one of the [32]global concern and major challenges of the future of world and international law enforcement.

As [33]ICT has become even more prevalent, aspects of cybercrime will feature in all forms of criminal behavior, even those matters currently regarded as more traditional offences. It already features in many international crimes involving drug trafficking, people smuggling, terrorism and money laundering. Digital evidence will become more common, even in traditional crimes, and we must be prepared to investigate with this new challenge. Law enforcement agencies around the world are working together to develop new methods of investigation and new forensic methodologies to respond to cybercrime in order to ensure safety and security on the Internet.

New skills, technologies and investigative techniques, applied in a global context, will be required to detect, prevent cybercrime. As the cybercrime is growing, we need to respond in much more quick way, and challenging technical and legal complexities. Innovative responses include cybercops, cyber court and cyber judges which are specialized in cyber law but eventually require to overcome the significant jurisdictional issues as mentioned in research paper.

Necessitated large scale amendment in information technology act-

[32] Neelesh Jain, cybercrime changing everything – an empirical study, international journal of computer applications (Feb 01, 2014), http://www.rspublication.com/ijca/ijca_index.htm.
[33] Pieter Kleve, Richard De Mulder, Kees van Noortwijk, The definition of ICT Crime, ScienceDirect (23 March 2011), https://www.sciencedirect.com/science/article/abs/pii/S0267364911000057.

Further analyzing my research, I should these changes should be made in our current system-

i. The law enforcement agencies are facing noncorporation from intermediaries like social media platforms, bankers, crypto currency exchanges, owner of various servers due to which reaching out to cyber criminals has become a challenging task like to investigate the details of profiles committing cognizable offence on such platforms. Though sec 69 of IT act makes it compulsory for these intermediaries to assist the government yet the law enforcement agencies mostly face non corporation and their investigation reaches no end.
ii. More awareness program should be organized by government and educational institutions to make the Make the women and children aware about the aspects of cyber like and legal remedies for the victims of cybercrime and preventive measures to be taken to avoid getting prey of cybercrime.
iii. The jurisdictional area of investigation should be shifted from the location of the victim to that of the accused for faster investigation.

For example, A resides in Dehradun and has been defrauded by a criminal who is operating Delhi and A files a complaint in Dehradun, even if Dehradun police wants to investigate the case that will take a lot of time and hard work and ultimately when the criminals are caught the trials will take place in Delhi. So, it's better that the complaint at initial stage should be transferred to the criminal's jurisdiction.

iv. Imposing civil penalties and making the offence non bailable. Most of the cybercrimes are punishable only for 3 years and the minimal amount of fine even for crimes like sextortion, ransomware attacks, cyber warfare and slanderous mala fide.
v. AI morphed photos and videos should be made deleted at instant and should not have a lengthy process
vi. For dark net crimes where one can hire contract killer, sell narcotics with anonymity and cryptocurrency frauds have no specific mention in information technology act
vii. According to sec 78 and 80 of IT act only officer rank inspectors and officers of above rank shall investigate cyber offences and have the power of search and seizure. There is substantial shortage of officers for investigation of cybercrime and those who are trained well so police officers of the rank of sub inspector may also be authorized to investigate cyber offence.

BURNISHED LAW JOURNAL