

SOUTH ASIAN JOURNAL OF MANAGEMENT RESEARCH (SAJMR)

Volume 11 Number 1

October 2021

Special Issue on Intellectual Property Rights (I.P.R.)

Contents

Editorial Note

A Short Overview of Intellectual Property 858
Raghavendra Angara, PhD

Intellectual Property Rights & Cyber Crime 864
Mr. Amit A. Dongare

**Recent Trends And Challenges In Teaching
Intellectual Property** 874
Dr. Amardeep D. Jadhav

**Intellectual Property Rights Vis-a -Vis Constitutional Rights
With Special Reference to Copyright** 881
Sureshbabu Narayana Rayadurgam

An Overview Of Geographical Indications In India 889
Nuzhatparveen Ganihar, S.R Mulla, S.G.Gollagi and Satyanarayana C.

**An Overview Of Intellectual Property Rights And Its
Importance** 892
Prof. Sayed Wajid Peerzade, Prof. Gulbahar Killedar

Editors

Dr. T. V. G. Sarma, Prof. Amar D. Ekal & Prof. Sayed Wajid Peerzade



**Chhatrapati Shahu Institute of Business
Education & Research (CSIBER)**

(An Autonomous Institute)

University Road, Kolhapur-416004, Maharashtra State, India.

SOUTH ASIAN JOURNAL OF MANGEMENT RESEARCH (SAJMR)

ISSN 0974-763X

(An International Peer Reviewed Research Journal)

Published by

Chhatrapati Shahu Institute of Business Education & Research (CSIBER)

University Road, Kolhapur - 416 004, Maharashtra, India

Contact: 91-231-2535706/07 Fax: 91-231-2535708 Website: www.siberindia.co.in

Email: sajmr@siberindia.co.in. sifersajmr@gmail.com



- *Patron*
Late Dr. A. D. Shinde
- *Editor*
Dr. P. G. Naik
CSIBER, Kolhapur, India
- *Editorial Board*
Dr. Babu Thomas
Sr. Aloysius Inst. of Mgt. & IT, Mangalore, India
Dr. Francisco J. L. S. Diniz
CETRAD, Portugal
Dr. R. V. Kulkarni
CSIBER, Kolhapur, India
Dr. R. A. Shinde
CSIBER, Kolhapur, India
Dr. Paul B. Carr
Regent University, USA
Dr. M. M. Ali
CSIBER, Kolhapur, India
Dr. D. K. Lal Das
RSSW, Hyderabad, India
Dr. M. Nandkumar Mekoth
Goa University, Goa, India
Dr. Babu Zachariah
CSIBER, Kolhapur, India
Dr. Gary Owens
CERAR, Australia
Dr. K. Pradeepkumar
CSIBER, Kolhapur, India
Dr. R. M. Bhajracharya
Kathmandu University, Nepal
Dr. P. R. Puranik
NMU, Jalgaon, India
Prof. K. R. R. Mahanama
Colombo University, Sri Eanka
Dr. Yogesh B. Patil
Symbolis Inst. of International Business Pune,
India
Dr. Rajendra Naragundkar
IFM, Bangalore, India
Dr. K. V. M. Varambally
Manipal Institute of Management, India
Dr. R. L. Hyderabad
Karnataka University, India
Dr. B. U. Dhandra
Gulbarga University, India
Dr. A. D. Jadhav
CSIBER, Kolhapur
Dr. Praveen P. Chavan
CSIBER, Kolhapur
Dr. D. N. Valvi
CSIBER, Kolhapur
Dr. Rasiya Padalkar
CSIBER, Kolhapur
■ **Dr. V. Ravi Kishore Kumar**
CSIBER, Kolhapur, India

Intellectual Property Rights and Cyber Crime

Mr. Amit A. Dongare

Ph.D Scholar, L.N.M.L. Maharashtra Institute of Labour Studies, Mumbai University.
(amit.a.dongare@gmail.com)

ABSTRACT: This article explores the interlinked between Cyber Crime & infringement of Intellectual Property rights. Generally people has mentality that they want everything at free of cost i.e. free antivirus, free software, free wifi internet, free latest movies, serials, Netflix episodes, etc but free version of such things on internet & other online media platform is the trapped set by cyber hackers to hacked data & information in laptop, PC or smartphone. Such people not only infringed the copyright work of owner but also they become victim of cybercrime. Due to less awareness & knowledge about cyber safety & security; people gets easily trapped in cyber criminals illegal activities & become a victim & lose their hard earned money, personal data & information. This article mentioned cyber security tips & precautionary measures to protect Intellectual Property work. This article is useful for all people who use digital electronics instrument, smartphone, computer, tab, internet, also who do work from home; this article is useful to safe personal data, information & money from cyber criminals.

Keywords: Cyber Crime, Cyber Security

1.0 INTRODUCTION:

Latest web based technology, smartphone, internet has increased our capacity to do financial transactions, e-commerce & quick electronic business transaction. The new internet culture with cyber space has changed the function of modern business which include online advertising, online ordering, online shopping, online education, publishing, banking, entertainment, investment, auction, professional services, etc. Internet has reached globally so it provides unlimited market to the owner of Intellectual Property. But it has negative side also because internet also provides expended opportunities to criminals to infringe the rights of owner. The Intellectual Property owners must be aware of new forms of infringement of Intellectual Property that occurs due to new internet technology. World Intellectual Property Organisation WIPO & World Trade Organisation WTO gives protection to Intellectual Property by maintaining balance between return on investment in knowledge to IP owner & giving unrestricted access, benefits of knowledge to the

IP user.

Cyber crimes which are related with IPR includes software piracy, copyright infringement, cyber-squatting, domain name registration, web site related defacement.

There are many reasons due to which cybercrime rates has increased which includes less knowledge of cyber safety among public, less police manpower and less cyber cells to find out cyber criminals, also latest & advance technology are using by cyber criminals & creating new tricks & tactics to trap people.

Cyber criminals are taking disadvantage of covid lockdown period & by using name of well known company, they posted fake advertisement on social media to sell N95 face mask, spreading fake links of covid vaccine registration & oxygen cylinder availability, etc. people pay advance money but didn't receive materials & when they asked for refund of money, criminals are given many reasons & again cheated the victim. Many cases has been registered in Mumbai police station regarding using well-known companies name for fake advertisement on social media.

Cyber peace foundation has find out that Chinese hackers are spreading fake message on Whats App about 'Corona Subsidy'. Message consists of people who are suffering financial problem due to pandemic will get financial subsidy from 'corona foundation'. To avail financial subsidy, people open the Whats App message & click on links which collects all banking & personal information. People gets trapped in this new type of tricks & become a victim of cyber crime.

Police has noticed that cyber criminals contacted relatives of covid patients or circulate fake links of availability of Remdisvir injection & Tocilizumab injection on social media & pretend them as a dealer or distributor or representative of Cipla Pharma Company & give them false promised to supply Remdisvir injection & Tocilizumab injection after paying online advance payment for it. But after payment victim didn't get these lifesaving drugs. Cases has been reported in police station that many relatives of covid patients trapped in this new type of cybercrime.

Cases of cyber espionage increased: - As per 'Fireeye Mandiant Services company' special report of 'M-trends 2021' mentioned 'Cyber threats against organisation who are working with COVID-19 information & research'. Mandian threat intelligence group tracked activities of hackers who are doing cyber espionage campaigns. Cyber threat groups in countries like Vietnam, China, North Korea, Iran & Russia are more active in cyber espionage campaigns. These cyber threat groups are targeting information & data of Covid-19 vaccine, treatment data, research & response data, etc. Confidential medical treatment data & information comes under intellectual property. These hackers targeted World Health Organisation office, pharmaceutical companies, healthcare, medical research & similar organisation, also targeted government offices, education, aerospace & defense, transportation, public & nonprofit

sector of other countries. Such cyber threats group also attacked on India's Corona vaccine manufacturing firm like Serum Institute, Bharat Biotech Company during the month of March 2021.

2.0 IPR & Cyber Crime

2.1.1. Copyright

Copyright is a unique kind of Intellectual Property Rights; also it is called as bundle of rights. Copyright consists of a different rights in the same copyrighted work which are the right of publication in magazines, journals & newspapers, the right of dramatic & cinematographic versions, the right of translation, the right of abridgement, the right of public performance, the recording right, the right of broadcasting, the right of reproduction.

Section 14 of The Copyright Act 1957 defines the term 'Copyright'- it's an exclusive right which authorise owner of the work to do following acts in respect of a work or any substantial part thereof which includes:-

a) In respect of literary, dramatic & musical work – to reproduce the work in any material form, to issue copies of the work to the public, to perform the work in public or communicate to the public, to make any sound recording or cinematographic film, translation or adaptation of work

b) In the case of computer Programme- to sell, give on commercial rental

c) In the case of an artistic work- to reproduce the work in any material form, to communicate the work to the public, to issue copies of the work to the public, to include work in the cinematographic film, to make adaptation of work,

d) In the case of cinematographic film- to make a copy of the film, to sell or give on commercial rental copy of the film, to communicate film to the public

e) In the case of sound recording – to make sound recording & store of it in any medium, to sell or give on commercial rental any copy of the sound recording, to communicate the sound

recording to the public.

2.1.2. Copyright Violation:

Publishing or using any painting, book, software, website or written document; without taking written permission from copyright owner which falls under copyright violation.

If someone illegally create or publish or sell it or make it available on internet duplicate copy of copyrighted movie, song, software, CD or DVD, blue ray disk then it comes under violation of copyright. Using or making some changes or modification in copyrighted owner's poem, song, article, music, or invention & using such copyrighted material in own name, which falls under violation of copyright.

Law relating to Copyright Violation:

Copyright Act, 1957, Trademark Act, 1999, Indian Penal Code 1860, Information Technology Act, 2000 are applicable for violation of copyright.

Section 51 of the Copyright Act, 1957 enumerates when copyright shall be deemed to be infringed i.e. infringement of copyright, when any person without the permission of the owner or the Registrar of the Copyright does anything act which he is not legally liable to do or when any person makes for sells, hires, or sells or distributes or exhibits in public or imports into India or lets for hire any infringing copies of the work, resulted in the infringement of the copyright in the work.

Chapter 13, Section 63, of the Copyright Act, 1957 mentioned offences of infringement of copyright- any person who knowingly infringes or abets the infringement of the copyright in a work or any other right conferred

by the act shall be punishable for imprisonment for minimum six months to maximum three years & with fine fifty thousand rupees to two lakh rupees.

Section 63 (A) mentioned enhanced penalty on second & subsequent convictions which is imprisonment for one year to three years & fine of one lakh rupees to two lakh rupees.

Section 63(B) mentioned if any person knowingly makes use of an infringing copy of computer Programme then he shall be punishable with imprisonment for a term of minimum seven days to maximum three years & with fine of fifty thousand rupees to two lakh rupees.

Section 420 of Indian Penal Code 1860 is applicable for software piracy which is cheating & dishonestly inducing delivery of property. Such person shall be punishable with imprisonment extend to seven years & shall also liable for fine. It's a non-bailable offence.

Section 405 of The Indian Penal Code 1860; which mentioned 'Criminal breach of trust' is also applicable for infringement of copyright work.

2.1.3. Sat-Isabgol case of violation of Copyright & Trademark

The Sidhpur Sat-Isabgol Factory, a partnership firm registered under the partnership Act situates at Sidhpur, Patan, Gujrat are the registered proprietors of the Trademark/labels of "B.G. Telephone brand Sat-Isabgol" with wide registration number 477558 & are the first adopter, user & originator of the said trademark & label. Label is also protected under the Copyright Act, 1957.



Said company filed a suit against the firm named Ranakpur Sat-Isabgol vide TM suit no 28/2018 before the commercial court of Ahmedabad, where the Hon. Court had restrained the said Ranakpur Sat-Isabgol firm from using the identical & similar label. But then also Ranakpur Sat-Isabgol firm flouted the injunction order of the commercial court of Ahmedabad & started using illegally adopted label which amounts to contempt of court. The police authorities have also seized the goods with the infringing labels from the retailers at Thane, Maharashtra. The Sidhpur Sat-Isabgol Factory has taken criminal as well as civil action against the retailers, wholesalers, distributors, traders whosoever engaged in infringing activities.

2.1.4 Software Piracy

Software piracy means it is an act of stealing, copying, installation, distributing, modifying or selling of legally protected software.

Software piracy has now become worldwide issue & industry is facing huge financial loss. It hinders the profit & success of the software industry nationwide & globally. According to the 2018 Global software survey 37% software installed in the computer, laptop, tab are unlicensed software. Online piracy or internet piracy happens when illegal software is download, sold, share or acquired through internet.

Consequences of software piracy are there is high risk of infecting computer, laptop with malware, virus & adware which compromised all data & information in the computer, it slowed down the computer, & user will face legal repercussion due to infringement of copyright.

Law relating to software Piracy:

- Section 66 of the Information Technology Act, 2000 (Amendment Act 2008) mentioned punishment for Computer Related Offences including software piracy. If any person dishonestly or fraudulently does any act under section 43 of the act then such person shall

be punishable with imprisonment up to 3 years or with fine up to 5 lakh rupees or with both. It's a bailable offence.

- Section 63(B) of Copyright Act, 1957 mentioned knowing use of infringing copy of computer programme to be an offence & such person shall be punishable with imprisonment of minimum 7 days which may extend to maximum 3 years & with fine of minimum fifty thousand rupees to maximum 2 lakh rupees. It's a bailable offence.

- Section 420 of Indian Penal Code 1860 is applicable for software piracy which is cheating & dishonestly inducing delivery of property. Such person shall be punishable with imprisonment extend to seven years & shall also liable for fine.

- Section 468 of Indian Penal Code 1860 mentioned forgery for the purpose of cheating. Forgery include document or electronic record forgery; such person shall be punishable with imprisonment extend to seven years & shall also liable for fine.

- Section 471 of Indian Penal Code 1860 mentioned whoever fraudulently or dishonestly uses as genuine any electronic record or document which he knows that it's forged such person shall be punishable under the law.

3.0. Infringement of Trade Marks

If a person other than registered proprietor or owner of the mark which is registered, uses the same mark or a deceptive similar mark such act comes under the infringement of Trade Mark.

Essentials of infringement are:-

- Taking essential feature of the mark or taking whole of the mark as it is or making a few additions or alterations in original registered trade mark

- Infringing trade mark must be used for the trade, business purpose

- Infringing trade mark must be printed & publish it in advertisement, invoice or bills.

- Oral use of trade mark is not comes under infringement.

3.1.1 Case study of Covishield Trademark of Serum Institute of India (SII), Pune:

Serum Institute of India (SII) in Pune, Maharashtra is producing corona virus vaccine named Covishield. On 4th January 2021 Cutis-Biotech, a pharmaceutical firm based at Nanded, Maharashtra files a suit in the civil court in Pune claiming Covishield is their brandname & sought to restrain Serum Institute of India from using this trademark & seeking injunction against the use of 'Covishield' trademark. SII had told to court that two companies are operate in different product categories & there is no scope of confusion of using the trademark Covishield. Pune Court rejects the application of Cutis-Biotech. Then they appeal in the Bombay High Court, But Bombay High Court also dismissed Cutis-Biotech plea seeking to restrain SII from using trademark 'Covishield'. The Hon'ble High Court has held that 'Covishield' is a vaccine to counter Coronavirus is now widely known. A temporary injunction directing Serum institute to discontinue the use of mark 'Covishield' for its vaccine will cause confusion and disruption in the vaccine administration Programme of the State. In this case, thus, the grant of an injunction would have large scale ramifications traversing beyond the parties to the suit."

4.0 Domain Names in IPR

In the new world of e-commerce, to promote business & to reach customers, it's important for company to have an address in the cyberspace i.e. company must have registered under a particular domain name & must have its own website. The Domain Name System (DNS) is helpful for company to conduct online transactions & make it easily accessible on the internet. The domain name played important function of showing companies recognitions, goodwill in the marketplace.

Satyam Infoway Ltd. Vs Siffynet Solution (P) Ltd.(2004) 6 SCC 145:(2004) 28 PTC 566 in this case the court held that, the use of the same or similar domain name may lead to user

accessing one domain name instead of another. Internet domain names are subject to the same legal norms as applicable to other Intellectual Property such as Trade Mark. There is no resolution in India which working on dispute resolution in connection with domain names. The Trademarks Act, 1999 is not extraterritorial as well as it's insufficient to protect domain names within the country.

4.1.0 Cyber Squatting

Cyber Squatting means buying an internet domain name & sell it to other person, business or organisation with intention to make a profit. To sell a domain name to the real owner of an identical or similar trademark is comes under infringement of trademark. The practice of Cyber Squatting is abusive. United States federal law known as the 'Anti Cybersquatting Consumer Protection Act' (ACPA) protects true owner of the domain name.

5.0. Website Related Defacement:

Website defacement is an attack on genuine or copyrighted website that changes the visual appearance, small changes in trademark, name of website or the webpage. Hackers do website defacement to replace the hosted website with one of their own.

Unexpected changes in website can mean a security compromise & called as defacement attack. Unauthorised access is the common cause of defacement attack.

Web Hijacking means taking forceful, illegal & without permission control of another persons website. In such kind of crime the actual owner of the website loses control over his website & its contents.

5.1.1 Law relating to website defacement:

- Section 65 of the Information Technology Act, 2000 (Amendment Act 2008) mentioned Tampering Computer Source Documents- Whoever knowingly or intentionally does act or causes another to do acts of conceals, destroys or alters any computer source code, computer commands, design & layout & programme analysis of computer

resource or computer system or computer network such person shall be punishable with up to 3 years of imprisonment or with fine extended up to two lakhs rupees or with both. It's a cognizable offence & Bailable offence.

- Indian Penal Code 1860, Section 463, Whoever makes or create any false documents or electronic record with intention to cause damage or intention to cause injury to any targeted person, group of person, to public or to support any claim or title or property or to enter in any contract or with intention to commit fraud or forgery is crime under IPC, 1860

- Indian Penal Code 1860, section 464, Making a False document- a) Makes, signs, seals or executes a document or part of a document. b) Makes or transmits any electronic record or part of any electronic record. c) Affixes any electronic signature on any electronic

records. d) Makes any mark denoting the execution of a document or authenticity of the electronic signature.

- Indian Penal Code 1860, section 468, Forgery for purpose of cheating- Whoever commits forgery, intending that such forged document or electronic record is used for the purpose of cheating; shall be punished with imprisonment up to 7 years or shall also liable for fine.

- Indian Penal Code 1860, Section 469, Forgery for purpose of harming reputation- Whoever commits forgery, intending that forged document or electronic record shall harm the reputation of any party & knowing that it is used for that purpose only; in such case such person shall be punished with imprisonment up to 3 years or with fine.

6.0 CYBER CRIME STATISTICS OF MUMBAI CITY:

Year	2019	2020
Total number of cybercrimes registered cases	2,225	2,435
Cases detected (case detected percentage)	284 (12.76%)	207 (8.5%)

Source: Hindustan times, 'Beware Mumbai recorded more cybercrimes in 2020: Data' 19 January 2021, pg 1. Lokmat, 'Big challenge for Mumbai Police to stop cyber crimes' 22 January 2021, pg 1.

Above mentioned table shows that there were more cases registered of cybercrimes in the year 2020 than last year 2019; which shows cybercrime cases has increased during covid 19 lockdown period. Compare to year 2019, the case detected percentage is less in the year 2020. It means during Covid 19 lockdown period cases of cybercrimes has increased but detection ratio is lower than non-lockdown period.

Major 5 cybercrimes registered & detection in the year 2019 & year 2020 information list:

Sr. No	Types of Cyber crimes	Year 2019	Year 2020		
			Detected Cases	Registered cases	Detected Cases
1	Credit card fraud	775	40	558	21
2	Obscene Emails	239	104	247	91

3	Fake social media	61	23	30	8
4	Phishing/ Hacking	34	2	37	6
5	Spoofing Mail	26	1	14	1
6	'Other' Cyber Crimes includes sextortion (sexual exploitation by coercion), e-shopping fraud, fraudulent classifieds & job listings	1087	112	1545	78

Source: Hindustan times, 'Beware Mumbai recorded more cyber crimes in 2020: Data' 19 January 2021,pg 1.

Lokmat, 'Big challenge for Mumbai Police to stop cyber crimes' 22 January 2021, pg 1

In above mentioned table statistics the cases of infringement of trademark, violation of copyrights by using Internet & Computer are also included in list of 'Other Cyber Crimes'.

Till December 2020, during corona lock down period, Cyber Cell of Maharashtra find out 14000 fake posts on social media and filed 400 cases of cybercrimes and took action on more than 100 peoples who did it. Cyber criminals created fake post on social media to defame government and police system, cyber criminals spread rumors and wrong information about corona virus on social media. Cyber cell find out more than 80000 fake accounts on social media which spread rumors and defame government.

7.0 SAFETY PRECAUTIONS AGAINST CYBER CRIMES

Use Strong password for Intellectual Property work:

- Keep Alpha-numeric with special character & include small & capital letters for making your password very strong. Strong passwords must have 8-10 characters.
- Change password on regular basis at least after every 90 days.
- Personal information should not be set as password.

Safety precautions from Software Piracy:

- Purchase original software from authorised dealer of company.
- Read properly terms & conditions of software before installing it in PC.

- Protect PC from paid version of authorised anti-virus.

- Install good genuine anti-virus software in computer & in mobile & keep updated it regularly. Never install pirated software or free version or demo version.

- There is need to create awareness about piracy of software & need to develop culture & promote ethics of being honest by using only original, authentic software.

- After evolution of information & technology & internet, piracy of software are become major problem to software industry.

Safety precautions of Copyright & Trademark Violation:

- Always ensure to search banks Branch/ office details/ toll- free number, etc in official bank website only. Never search for toll-free number or bank details in search engines.

- Do not download & install applications from untrusted sources there is high chances of copyright violation & cyber crime. Always download app from reputed application market. Always download apps & app updates from legitimates stores. Don't click on links for apps from emails or websites. Always use legitimate store to search & download app.

- Verify app permission & grant only that permission which have relevant context for the app's purpose. If the application is requesting for unnecessary permission, do not proceed with installation. Prior to installing any new application, always make sure to read reviews

on the App store or play store.

- Always verify & install authentic & genuine e-wallet apps from play store on smartphone. Because many similar apps of well-known e-commerce companies are available on internet which are created by hackers to trap people. Do not follow links shared on messages, email or other social media account to install e-wallet apps in smart phone.

- Cyber criminals use name of well-known e-commerce Company & create & send fake gift coupon/ lottery scams message on social media or internet. Never fall prey for fake gift coupon/ lottery scams. Never respond to such fake message/letters/ phone calls or any schemes or advertisement. Do not give any details or information to them.

Safety precautions to protect Domain name:

- Be sure to register domain name to the property entity. Domain name containing company's trademark should be registered to the same company.

- Use a reputable registrars to registered domain name.

- Lock the domain name.

- Use strong password to protect it.

- Register or renew domain name for longest period of time.

- Choose auto renew option so domain name registration will renew before it expires.

- Be aware of domain name scams.

Safety precautions against E-mail Phishing, Email Frauds, Email Hacking:

- Legitimate companies won't use email messages to ask for personal information. In such case contact company by phone. Don't click on links in these email messages.

- Do not believe any email message which mention to transfer funds urgently. In such case contact such person personally & cross verify email message.

Safety Precautions against social media challenge trends:

- During covid 19 lockdown period, social media like FB has started challenge to post photos of husband-wife, girlfriend-boyfriends, brother-sister, best friends, 10 years

old photos challenge etc & got tremendous responds from users. But FB sells such data to facial recognition & artificial intelligence companies & earned millions of dollars. Such photos also may be used by darkweb to sell illegal articles. Such photos may be utilized by criminals to create obscene videos.

- It is advisable to don't post personal information, personal photos, and videos on social media.

Cyber security tips for Work From Home employees:

- Don't use pirated or free or demo version of any software or antivirus in computer, laptop, smartphone.

- Keep software & browser updated & visit only https websites.

- Create secure Email & online accounts.

- Check social media privacy settings frequently.

- Create strong password for computer, email, social networking sites. Also keep strong password for computer/laptop, bluetooth, hotspot & Wi-Fi router. So no any stranger person can access it.

- Do not use open, unsecure, public Wi-Fi for online transaction or to access social networking sites or emails.

- Use paid version of Antivirus in your laptop/computer & update it regularly.

General Tips for Cyber Security:

- For online purchase, make sure that website is authentic & secure.

- Keep safe from phony messages/ spam messages. Fraudulent messages are misspellings, poor grammar, odd phrasing, web sites address with strange extensions. Phishing messages tell you to act quickly to keep account alive, & urge customer to provide information.

- Educate children & talk freely to them about cyber security & internet safety.

- Protect computer by using security software such as Fire wall & Anti-virus software.

- Secure your mobile/smartphone. Download applications from only trusted sources only.

- Install the latest operating systems in your device eg. windows, linux, mac, etc. Use only paid version of operating system & don't use free version or pirated version of application software.

- Do not use public or free Wi-Fi to download any applications or updates any software.

- Protect your e-identity means personal information on social media.

- Beware of fake social media accounts! Not all the accounts are real and not all information provided on accounts are true; so verify information as well as profile.

Know What To Do If You Become A Victim:

- If you become a victim of cybercrime, then firstly contact bank or service provider & block your bank account. Or someone theft your smartphone then contact service provider & block your sim card network.

- Contact Cyber police station / cyber crime cells that has the jurisdiction over your residence or office premises & file written cyber complaint. Online portals are also available to register cyber crime complaints. At the national level '<https://cybercrime.gov.in>'

- There has provision to report cyber crime by dialing the help line number 155260.

- In case you receive any fraud SMS, e-mail, link, phone call asking for any sensitive personal as well as banking information then immediately report it on cyber's web portal by visiting 'www.reportphishing.in'

- In absence of cyber police station or a cyber cell, victims can approach to high ranking police officer in their district like superintendent of police or deputy commissioner of police.

- Collect bank statements when you face bank fraud related cyber crime.

- If you received phishing email or faced problem of Email Hacking then save the received emails in pdf format or take the screenshot, note down or copy the full email headers details of phishing email. If phishing email has an attachments then save such attachments as evidence. Preserve the original evidence. Do not delete emails, email header,

screenshot attachments, etc. These documents are useful for police as an evidence.

- Report any adverse activity or regarding any unwanted behaviour to CERT-IN on their email address- 'incident@cert-in.org.in'. Or on helpdesk number - +91 1800 11 4949. Provide details of time of occurrence of the incident, information related to affected system/ network & symptoms observed while reporting incident.

8.0 Concluding Remarks:-

This article, which is based on cyber safety of Intellectual Property work. The entire world is facing problem of corona virus epidemic. GDP rate of India in the year 2019 was 4.18% & in the year 2020 was -7.97% which shows that during covid pandemic situation, India is facing problem of economic recession. On 23rd July 2021, 161st report on 'Review of Intellectual Property Rights Regime in India' presented in parliament which has mentioned during corona epidemic period Europe had earned 65 billion euro (sale value) by selling Geographical Indication (GI) products in international market. Last year China had filed 15 lakhs patents, 80 lakhs trademarks, 7.5 lakhs industrial design applications & 7000 GI applications & last year India filed 60,000 patents, 3.5 lakhs trademarks, 15000 industrial design applications, 370 GI applications. Percentage of Intellectual Property in GDP of developed countries is high. India is moving towards from developing countries to developed countries but for that India not only has to increase Intellectual Property work like Patents, Copyright, Trademark & GI but also need to protect their Intellectual Property work from infringement & violation.

Cyber criminals are targeting Intellectual property work of well known companies & created fake websites, links, messages which looks like genuine to trap people. For example fake annual sale or gift coupons of Amazon, Flipkart, Facebook, Dmart are created to lure the people. There is only solution for this problem is to create awareness among people about cyber crime & cyber safety. This article mentions precautionary measures for various cyber crimes related Intellectual Property work.

Also it has mentioned what to do after become victim of cybercrime. Various non-governmental organizations like DLAI & INTERPOL are taking leading role to create awareness among people. INTERPOL are providing technical help to their member countries government to solve cases of cyber crimes as well as helping to transfer data of crimes & criminals between countries.

NOTES:

1) The world is already entered in technology era. Day by day new technology comes into the market & replaced by old one. There is inclusive growth of technology; not only rich people even middle class or poor people are also using latest electronic devices.

2) Intellectual property owner needs to update with latest technology to avoid infringement of their intellectual work.

3) Intellectual property owner has to be updated with cyber security measures to safeguard their Intellectual property work.

4) Police department, few Banks, Security & Exchange Board of India, cyber experts are creating awareness among general public related to cyber safety.

5) Awareness about cyber crime & cyber safety is the only preventive measures available with us.

6) Data shows that there were more cases registered of cybercrimes in the year 2020 than last year 2019 but case detection percentage is lower in the year 2020 than 2019.

7) Keeping weak password to intellectual work, not using updated version of antivirus, using pirated version or free version or demo version of software & ignorance & less knowledge about cyber safety are the main causes of increasing rate of cyber crime & infringement of intellectual property work in the country.

REFERENCES:

• Ministry of Home Affairs Government of India, 'A Handbook for Adolescents/Students on cyber safety', PP 1-38.

• Ministry of Home Affairs Government of India, 'Online Safety Tips'; 'National Crime

Records Bureau Journal (NCRB)' New Delhi; Cybercrime reporting Portal, National Crime Records Bureau Journal (NCRB) New Delhi. Vol-I, (No1), October 2018, PP 1-4.

• Press release of Mumbai police Cyber cell on 30 April 2021- mumbaiipolice.gov.in

Books:-

• Bare Acts of Copyright Act, 1957, Trademark Act, 1999, Indian Penal Code 1860, Information Technology Act, 2000 (Amendment Act 2008)

• 'Cyber Law & Cyber crimes simplified' (2019) by Adv. Prashant Mali

• Cyber Laws & IT Protection, (2012) by Harish Chander

• Law relating to Intellectual Property by Dr. B.L.Wadehra

Newspaper News & Articles:-

• Hindustan times, 'Beware Mumbai recorded more cyber crimes in 2020:Data' 19 January 2021, pg 1.

• Lokmat, 'Be cautious if you take online information about vaccination' 24 December 2020, Pg 2

• Lokmat, '300 crores email passwords leaked', 7 February 2021, pg 10

• Lokmat, '14 lakhs fake posts, 400 crimes registered', 24 December 2020, Pg 3

• Loksatta Mumbai edition, 'Cyber safety during corona pandemic period', 20 November 2020, pg 4

• Loksatta, 'Online crime happens after working hours timing'; 4 March 2021, pg 4.

• Maharashtra Times, '93 lakhs cheating of online cyber crimes- behind masks' 11 February 2021, pg 1 & 3:

• Sakaal, 'Prosperity path of Intellectual Property' by Mr. Ganesh Hingmire; 31 July 2021. Pg.4

Websites:

• <https://cybercrime.gov.in/>

• <https://www.cert-in.org.in/>

• <https://ceir.gov.in>.

• <https://content.fireeye.com/m-trends/rpt-m-trends-2021>

• <https://nordpass.com/most-common-passwords-list/>