Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.
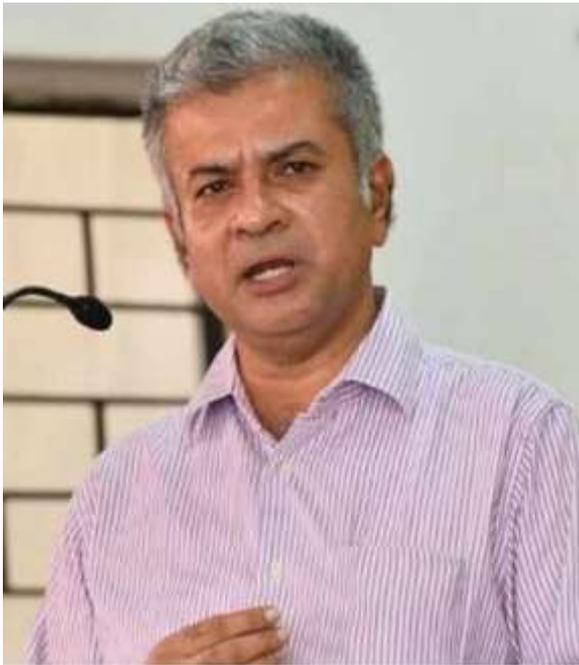
<u>DISCLAIMER</u>

EDITORIAL
TEAM

## Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.
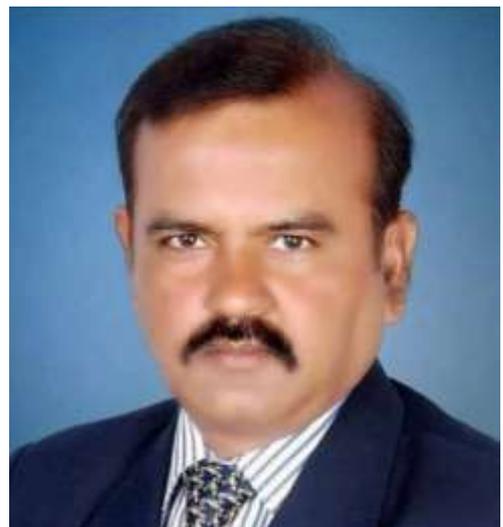
Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and

refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

THE VOLUME OF THE CONTENT BASED ON ONLINE FRAUDULENT

AUTHORED BY: ABIRAMI S, T.S.NANDHINI & R.KRITHIKA

Dhanalakshmi Srinivasan University, Samayapuram, Trichy.

Abstract

In this article we explain about online fraud in the state. who are all suffering from online fraud. There are some key aspects of fraudulent we give in this article, also we give types, punishment regarding, ratio of fraudulent, preventing from fraudulent. in this article we give some changes from scam. In this current society we use lots of technologies. The technology can be used in a positive or negative way. It is used in a positive way. It's useful for education, gaining knowledge and also earning. In a negative way we should face scam, online fraud etc... In the future we can live our lifestyle safe and secure. In this article we aim to protect and prevent online fraud.

INTRODUCTION

Cybercrime is a crime to commit illegal activities in online sources like computer, network, online database, hacking, bullying, sexortion etc.. It used to hack individual people's privacy. It also affects all children and adults. It is the biggest problem in this world. In the world of the era we all use technology in day to day life. There are different ways to use technology like positive or negative. In a positive way we use it for Education, knowledge gaining, earning, money oriented purposes etc.. But some persons are used in negative shades like to hack individual persons privacy, online money fraud, sex related issues etc... we aims who are all troubling from this online fraudulent to protect and prevent from this Cybercrimes. We implement some ideas to prevent cybercrimes.

Definition for cyber crime
- David's wall: Cybercrime refers to the use of computer technology to commit the commission of crimes, including those that are traditional in nature and that are unique to the digital environment.

- Peter: Cybercrime is a type of a crime that involves the use of computer technology to commit the offences, including fraud.
- Bruce Schneie: Cybercrime is the use of computers and the internet to commit crimes including identity theft.
- Kevin Mitnick: Cybercrime is the exploitation of computer systems and technology to commit illegal activities including social engineering and hacking.

Types of online fraudulent:-

- **Phishing:**

Phishing is a type of fraud. This fraud is done by an individual, not a group, but by a group. This phishing is done through a person's mobile phone or computer. Usually, an attacker attacks by sending an email or snatching the personal information to the user of the computer or mobile phone. The trick to get this personal information is using various technologies such as spam email, links,message, personal notification, texts etc ...

- Hacking:

hacking is an online fraudulent This hacking is the act of taking personal information of a person. This hacking is used to take personal communication or account details. hacking is very useful to take personal information of a person without his knowledge. This can be done by any means, if a person or a group of people use a computer to do this. There are many types of hacking Season hacking, personal data collection, account hacking, mobile hacking, cyber hacking, website In this hacking Dislodged by an OTP or PIN number It is a hacking of online fraud.

- Vishing:

Vishing is an online fraudulent activity. Another name for this type of activity is social engineering. The purpose of this vishing is to obtain personal information from an individual. It is done online. It can involve voice messages, phone calls, and voice recorders. This involves taking personal information from an individual, for example, a credit card number, account number, or sending a message claiming that a product has arrived and then withdrawing money from their account. This vishing is used for criminal activities.

- Account takeover fraud:

Account takeover fraud (Ato) is an online fraudulent activity, the purpose of this Account takeover fraud (Ato) is to hack another person's personal online account, in which the online account can be a personal account, email account, bank account. This is something that is done by another group or an individual without the knowledge of that individual. They will take everything they need from another person's account without the owner's permission.

There are having a different types of the of attacks, including phishing, malware attacks, social engineering, or data breaches...

- Online shopping:

Online shopping is that type of online fraudulent activity. This online scam is selling a product that does not exist and the customers who buy it lose money. This online scam has many types of websites, links, emails, social media ads, whatsapp messages, ect ... When people order a product, they will steal money from them. This online shopping is selling products at low prices and they will give advertisements. This is an online shopping.

- Lottery scam:

Lottery scams is a type of online fraudulent activity. This lottery scam is a message that comes as a message on the internet sites like email, phone call, whatsapp, etc. When we receive a message from any of these things, there will be large numbers in it, and it will be indicated that you have won. The purpose of this lottery scanning is to snatch money by saying advance fee. If you pay the advance fee then we will give you lottery money. It is a lottery scam.

- Dating scam:

Dating scam is a type of online fraud. This dating scam is about creating a fake profile. It can also be called a romance scam. This dating scam involves creating a personal profile on websites like Facebook, WhatsApp, Instagram, and through that, they will commit fraud. By creating this fake profile, they gain the affection and trust of another person and through that, they manipulate them into having a close and romantic relationship with them. It is a dating scam.

- Identify theft:

Identity theft is a type of online fraud. It is an online scam where a person who has made a mistake hides the mistake and leaves another person who has not made the mistake behind, so that the person who made the mistake can escape. This is identity theft.

- Internet fraud:

This internet fraud is a type of online scam. This internet scam is about knowing the personal details of another person. For example, hacking, phishing, phishing online ect... This internet fraud is generally covered in cybercrime. This helps to take all the personal details through a link and take out money without the owner's permission . This is taken for the apps etc . It is an internet fraud.

- Online harassment:

Online harassment is defined under the IT Act 2000 as any form of harassment that is done by an individual or a group of people repeatedly. This harassment can happen to women . After getting used to talking well on online platforms, they can be subjected to various types of sexual, social abuse, called online harassment.in this taken in a types of harrasment there are denigration, doxxing, exclusion, image based on the sexual abuse, mobbing, upskirting,

Trolling, trickery, sexting,internet pile on , masquerading ext. ..... Its is a online harassment

Ratio of cybercrimes in India

- India is among the most affected countries by cyberattacks and has also increased cybercrimes in recent years.
- Number of cyber attacks in 2023, India experienced over 79 million cyber attacks, which was a 15% increase from the previous year.
- The first quarter of 2024, over 500 million cyber attacks were blocked.
- 1.750 crore the India lost in 2024 first four months to cyber criminals
- The India recovery rate is too low. The recovery rate is 20%.
- In cybercrime, India takes the 10th rank of the world.The India met cyber fraud involving advance fee payment is a common type.

The punishment regarding of the cybercrimes:

1. The Information Technology Act 2000, also known as IT Act, deals with cybercrime and e-commerce. This act was implemented on 17 oct 2000, to provide legal recognition for electronic documents and facilitate e-governance.

2. Under IT Act 2000, extending punishment like individual guilty can be punished by 2 years or a fine extending one lakhs rupees. Moreover, section 66 provides, punishment for identity theft shall be punished extend three years or fine not extending two lakhs.

3. There are some penalties and imprisonment for cybercrimes. If penalty 2,00,000 fine and imprisonment 3 years for violation of privacy and tampering with computer source documents.

4. If the penalty is 10,00,000 fine and imprisonment 7 years for publishing or transmitting obscene material or containing sexually explicit acts etc.., in electronic form and child pornography.

5. The penalty is 5,00,000 for hacking and 1,00,000 for identity theft. They're not similar crimes. But both crimes have the same punishment. The punishment is 3 years for both hacking and identity theft.

- Preventing Of Cyber Crimes:

  We have some ideas to implement in this article that should alert people about such cybercrimes. The people are mostly involved in online shopping. There are many platforms regarding shopping bases. People should be aware that the platform is real or a scam. all online platforms must be approved by the government. all platforms will attach the government approved symbols in their logos.

- Online Harassment:

  Children who are not all 18 years old are prohibited from using the phone. Any online platform should not be approved to login their applications. The parents should not support the childrens to use the phone. The adults who are all 18 years old should be alert to use online platforms. they should not give any personal information to an unknown person. We should use Our knowledge to protect ourselves from these scams.

- prevent by individuals: educate yourself, learn about fraud schemes, use a strong password, protect the information.

- use strong password: We should use a different I'd and we should use different passwords in a letter or numbers.

- secure your computer prevent virus by infecting your computer by installing the regular update antivirus software: secure your mobile devices

- must aware from the mobile hackers and we must prevent the mobile devices from the hackers.

- protect your data: We must make a regular backup of all your important data.

- financial prevention: use secure payment processing, verify transactions, keep financial records sure.

Conclusion:

In this article, we conclude that people should be alert in such scams. We should not share our personal information with anyone. When we do any online shopping or download an app, we should read all the information that comes in it and then accept it. Similarly, if we receive a message from someone's number on our phone and ask for an OTP, we should not say anything. Only by doing all this can we protect ourselves from online fraud. We should use our knowledge to protect ourselves from these scams.

Reference:

- https://www.cisco.com/site/in/en/learn/topics/security/what-is-cybercrime.html#:~:text=C ybercrime%20is%20illegal%20activity%20involving,and%20instigate%20other%20d igit al%20attacks

- https://delhi-lawyers.in/blog/cybercrime-punishment-india

- https://www.eap-india.com/online-harassment-meaning-types-impact/

- https://m.economictimes.com/definition/hacking/amp

- https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams

- https://www.google.com/url?q=https://www.thehindu.com/sci-tech/technology/incidents- of-cyberattacks-on-india-may-reach-17-trillion-by-2047-study/article68810313.ece&usg =AOvVaw3QBMpoeccx9BT8zj9nCrf3

- https://law.lclark.edu/live/news/6855-what-is-online-fraud

- https://pcpc.gov.in/files/1.pdf

- https://timesofindia.indiatimes.com/gadgets-news/explained-what-is-online-shopping-sca m-and-how-to-stay-safe/articleshow/105906727.cms