ALL INDIA INSTITUTE OF MEDICAL SCIENCES, RAJKOT, INDIA

DEPARTMENT OF FORENSIC MEDICINE & TOXICOLOGY

E-MAGAZINE OCT-DEC 2022 VOL.1 ISSUE 3

# May I Help You!!!

## Cyber-crime & its forensic implications

**52,974**

Incidents of cyber-crime cases reported in India within 1 year

According to the NCRB data.

**National Cyber Crime Reporting Portal (Helpline Number - 1930)**

# What is cyber-crime?

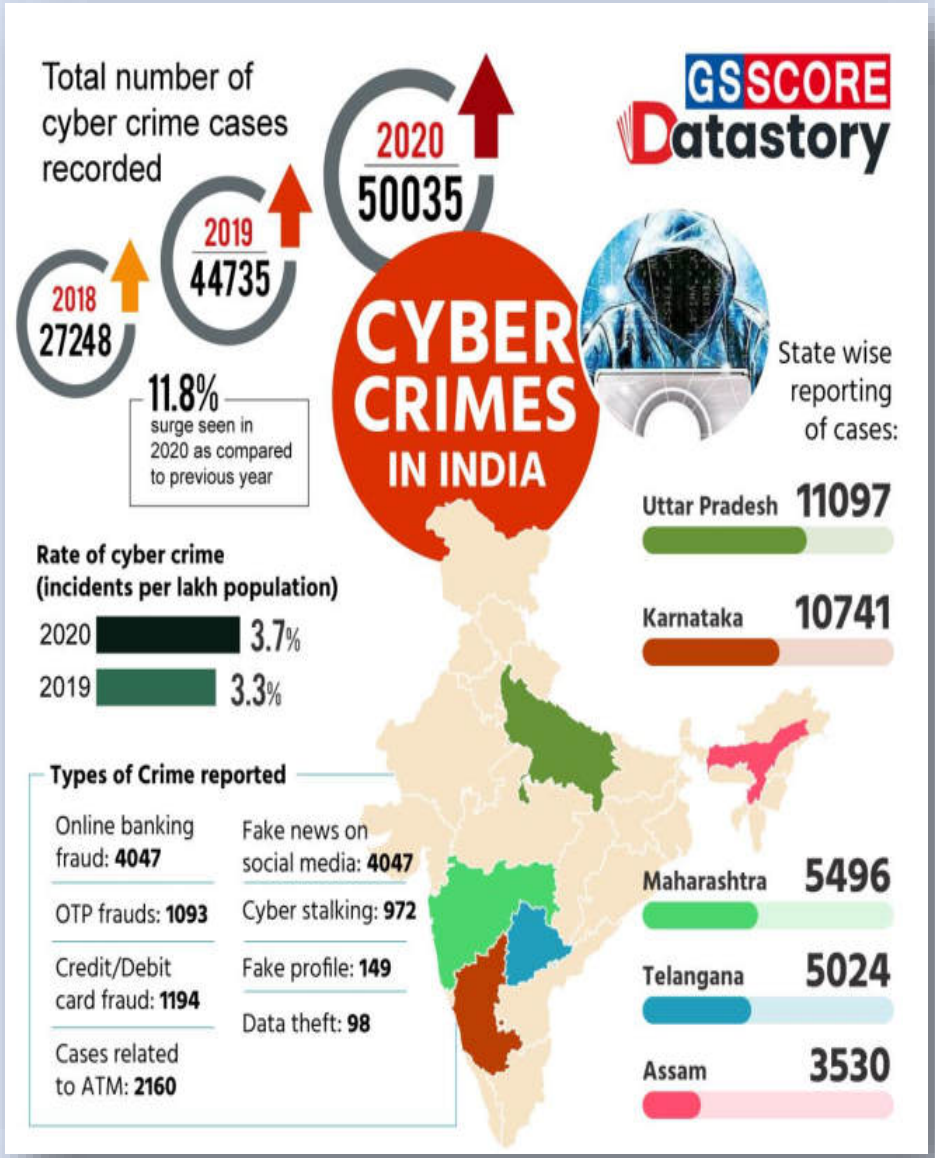
- Cyber-crime is an “unlawful act in which the computer system is used either a tool or a target or both “.
- Cyber-crime occurs when information technology is used to commit or conceal and offence.
- Cyber-crime is intentional and not accidental.

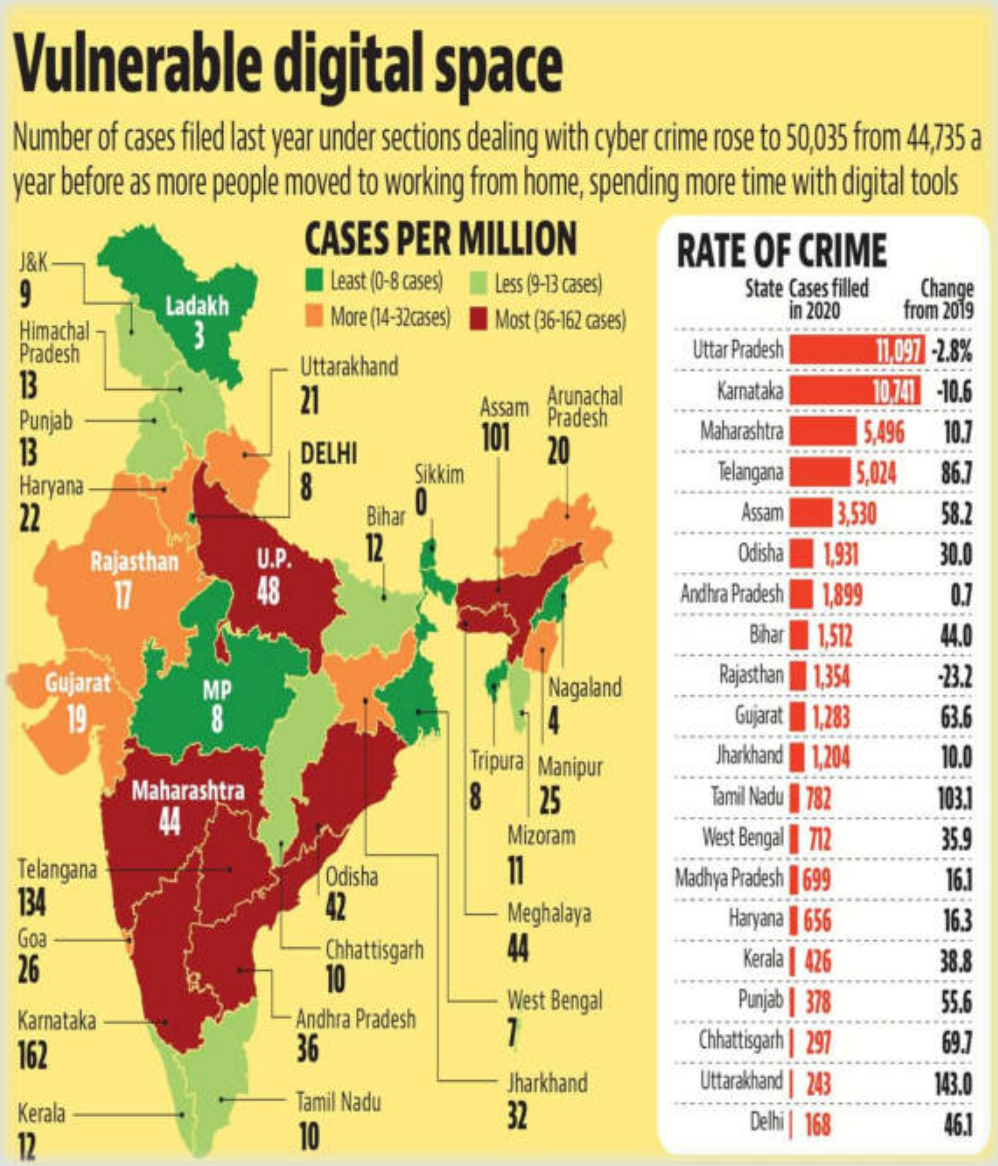

# Types of cyber-crime

Cybercrime ranges variety of activities. Cyber-crime can be basically divided into three major categories:

- **Cyber-crimes against persons** like harassment occur in cyberspace or through the use of cyberspace. Harassment can be sexual, racial, religious, or other.
- **Cyber-crimes against property** like computer wreckage (destruction of others' property), transmission of harmful programs, unauthorized trespassing, unauthorized possession of computer information.
- **Cyber- crimes against government** like Cyber terrorism.

# Cyber-crime statistics



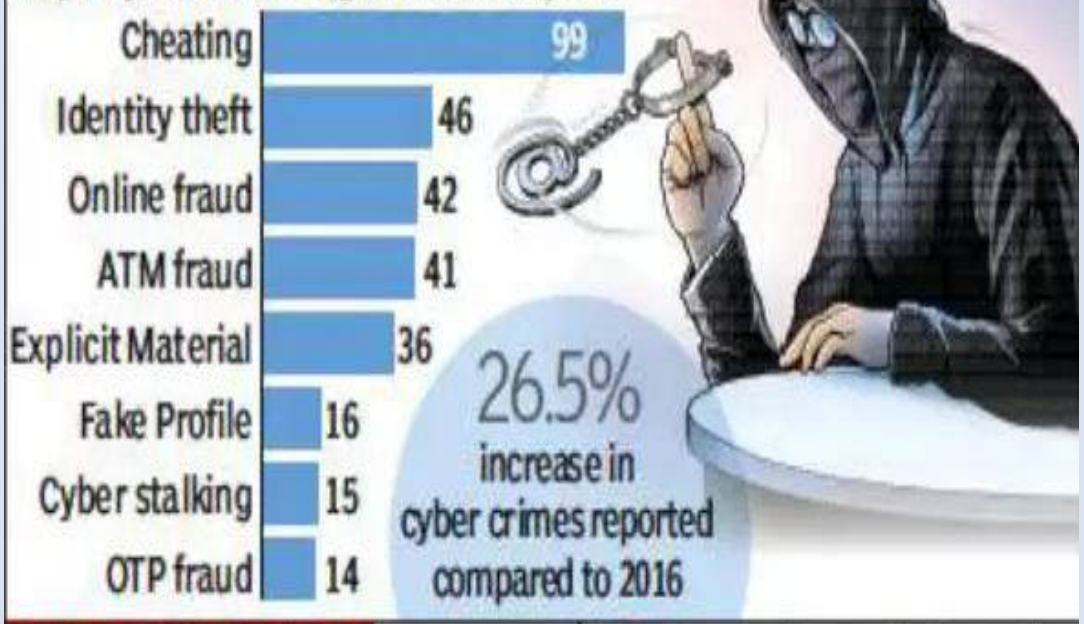
# Article of News-Paper

## THE PEGASUS PROJECT

- Paris-based media nonprofit Forbidden Stories and Amnesty International accessed a leaked database of thousands of phone numbers across the world targeted by a spyware called Pegasus
- They shared the data with global media organisations as part of a collaborative investigation called Pegasus Project
- An Israeli company called NSO Group makes Pegasus, a spyware capable of extracting data from a phone
- According to the report, at least 2 Union Cabinet ministers, 3 opposition leaders, a Constitutional authority, government officials, scientists and over 40 journalists in India were targeted

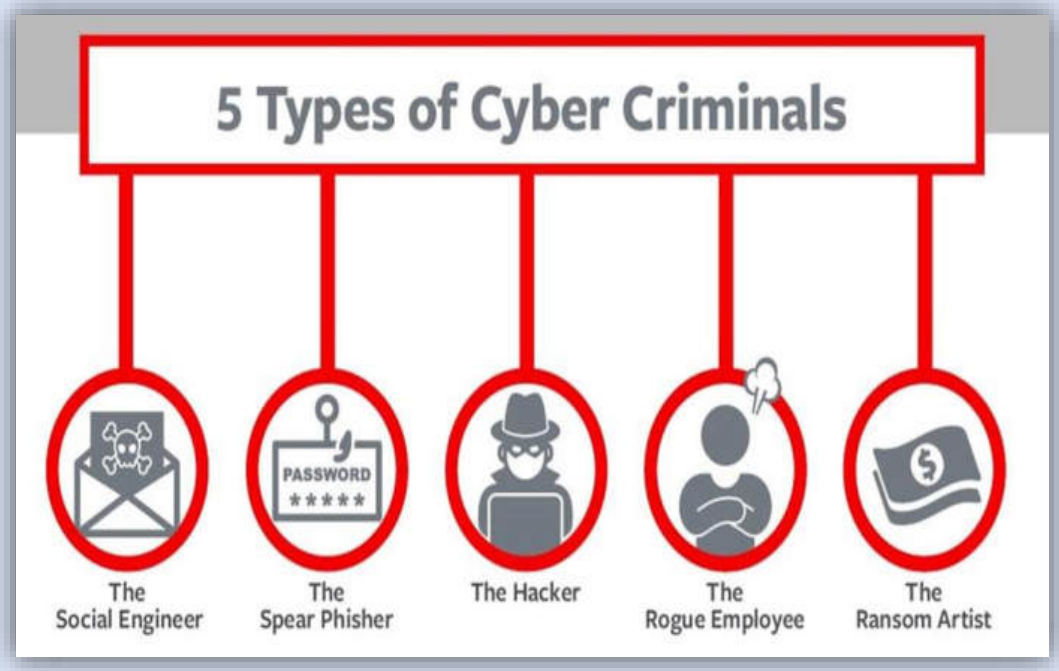
## BE SAFE ONLINE

**Major cyber crimes registered in Gujarat**

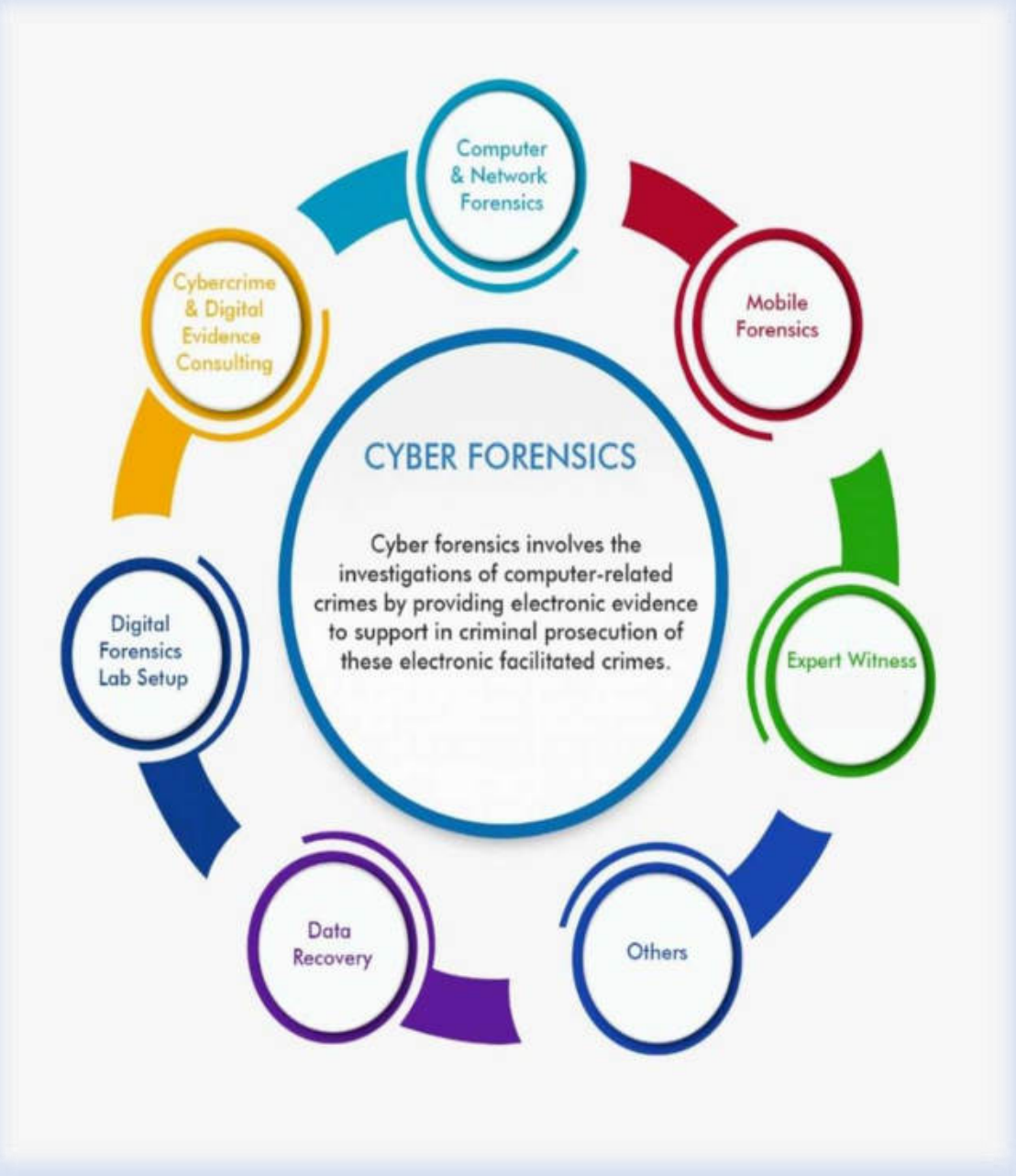



## THE CHEATED

- In October, Ahmedabad resident paid Rs 61,000 for getting a refund for a bad pizza as online cheats sent him a link and duped him off the money
- In September, a 20-year-old jilted lover from Gandhinagar was arrested for making fake profile of a girl and posting obscene pictures and messages
- In June, cyber cell arrested 7 accused for creating phishing websites that mimicked the income tax website and web pages of leading banks. When victims downloaded the mobile application, it gave fraudsters access to all personal details. They could extract information from victims' phones were 'active' or in 'sleep mode'



# Cyber Forensic Steps




## Steps of Digital Forensics

### *1. Identification*

First, find the evidence, noting where it is stored.

### *2. Preservation*

Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.

### *3. Analysis*

Next, reconstruct fragments of data and draw conclusions based on the evidence found.

### *4. Documentation*

Following that, create a record of all the data to recreate the crime scene.

### *5. Presentation*

Lastly, summarize and draw a conclusion.

# Preventative Measures

## DOS & DONTS

- In case you are a victim of cyber fraud, take screenshots of online transactions
- Inform police immediately about the cyber fraud so that quick action can be taken
- Do not click on any unknown link. It may forward you to a third-party application and you may fall prey to cybercrime

- Do not trust information or links received through bulk SMS service
- Contact the local office of your bank or telecom service company for required details
- Never share your details about UPI, Debit/Credit Cards and bank account with anyone
- In case you use internet banking, change your password regularly
- Do not share any OTP received on your phone with anyone
- Do not trust customer care numbers displayed by internet searches
- Always keep your social media profiles locked

Graphic: Utpal Chakraborty

## TAKE MEASURES BEFORE IT'S TOO LATE

India ranks **3rd** in cases of cyberbullying

City schools sit up as students post obscene memes on teachers online

The TOI story on Dec 19

### CATEGORIES OF CYBER CRIME BY KIDS

Cyberbullying | Digital piracy | Sexting

### HOW TO KEEP KIDS SAFE ON CYBER SPACE

- Use parental control software
- Place the computer in a busy area of the house
- Bookmark for safety and avoid downloads from unrecognized sources
- Set limits on late-night use; establish rules and take control
- Stay in the loop

"The problem is that a majority of such crimes has no criminal intent. They are seen as an extension of a prank. But children often don't realize the danger"

A POLICE OFFICER

## WHAT THE COURT SAID

THE SUPREME COURT STRUCK DOWN A PROVISION IN THE CYBER LAW WHICH PROVIDES POWER TO ARREST A PERSON FOR POSTING ALLEGEDLY OFFENSIVE CONTENT ONLINE

**THE PUBLIC'S** right to know is directly affected by Section 66A of the Information Technology Act. The provision "clearly affects" the right to freedom of speech and expression.

Terms like "annoying", "inconvenient" and "grossly offensive" used in the provision are vague as it is difficult for the law enforcement agency and the offender to know the ingredients of the offence.

When judicially trained minds can reach on different conclusions while going through the same content, then how is it possible for law enforcement agency and others to decide as to what is offensive and what is grossly offensive. What may be offensive to a person may not be offensive to the other. *(sic)*

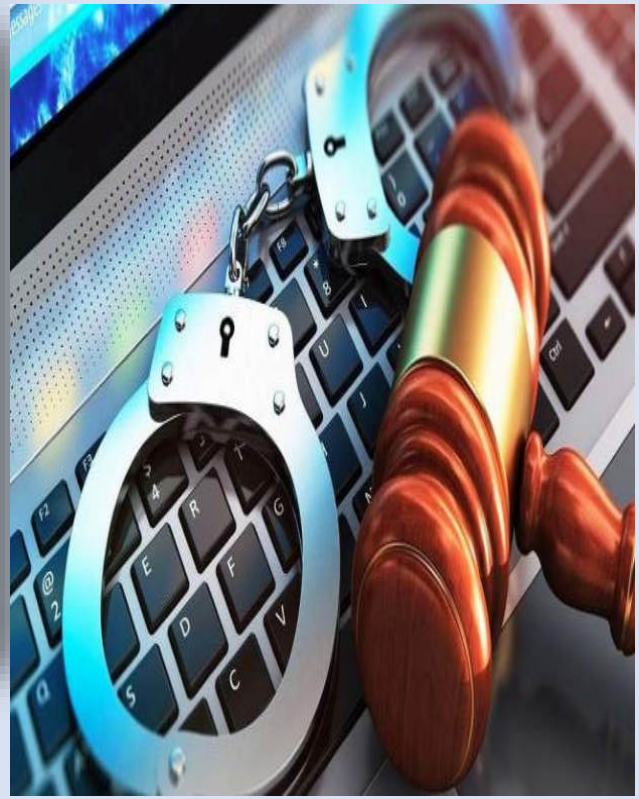
## THE CONTENTIOUS SECTION

**66A** Punishment for sending offensive messages through communication service, etc. Any person who sends, by means of a computer resource or a communication device —

**(a)** any information that is grossly offensive or has menacing character; or

**(b)** any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such a communication device,

**(c)** any electronic mail for the purpose of causing annoyance or inconvenience or to deceive the addressee, shall be punishable with imprisonment for a term which may extend to three years and with fine.



## Following are some of the penalties under cyber law in India

| Particulars | Penalties |
|---|---|
| Tempering with computer source documents | Up to 3 years imprisonment, or with fine of upto 2 lakh rupees or with both |
| Sending offensive messages through communication service. | Up to 3 years imprisonment, with fine |
| Violation of privacy. | Up to 3 years imprisonment, or with fine of upto 2 lakh rupees or with both |
| Publication for fraudulent purposes. | Maximum 2-year imprisonment, or with fine which may extend up to 1 lakh rupees or with both. |
| Publishing of absence information in electronic form. | Maximum 10-year imprisonment or with fine which may extend up to 2 lakh rupees or with both. |

# IPC Section 354 – D (Stalking)

Any man who—

- Follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
- Monitors the use by a woman of the internet, email or any other form of electronic communication, commits the offence of stalking.

## Criminal Law (Amendment Act, 2013)

| Offense | Punishment |
|---|---|
| Stalking | 1) Upto 3 years + Fine for first conviction<br>2) Upto 5 years + Fine for second or subsequent conviction |

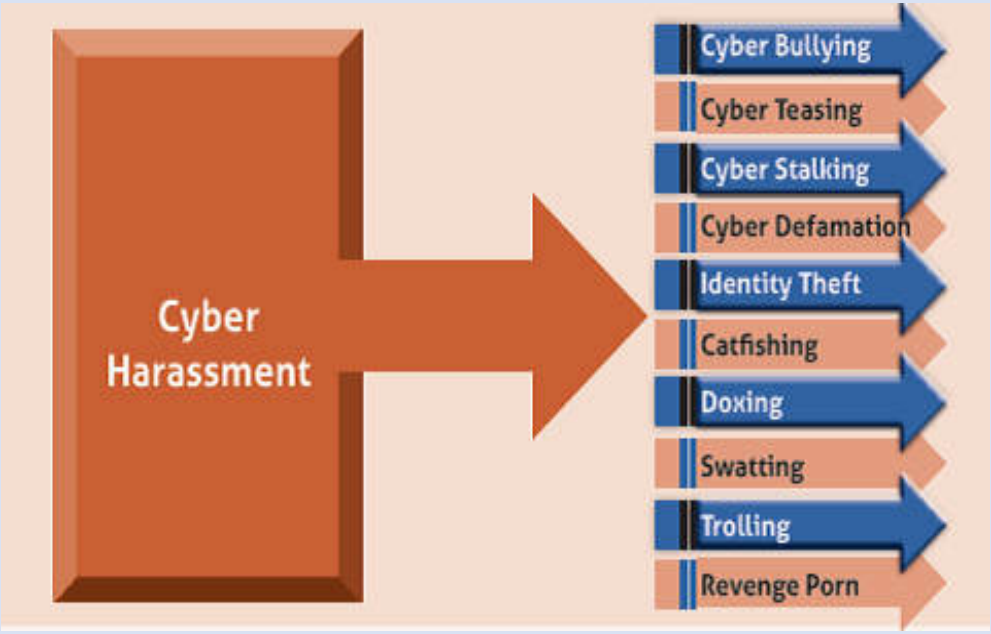
| Cognizable | Bail | Trial By |
|---|---|---|
| 1) Cognizable<br>2) Cognizable | 1) Bailable<br>2) Bailable | 1) Any Magistrate<br>2) Any Magistrate |

# Cyber harassment

Cyber harassment is perhaps the broadest form of cyber violence and involves a persistent and repeated course of conduct targeted at a specific person that is designed to and that causes severe emotional distress and often the fear of physical harm.

Cyber harassment is often targeted at women and girls and termed “cyber violence against women and girls” (CVAWG or Cyber VAWG) involving:

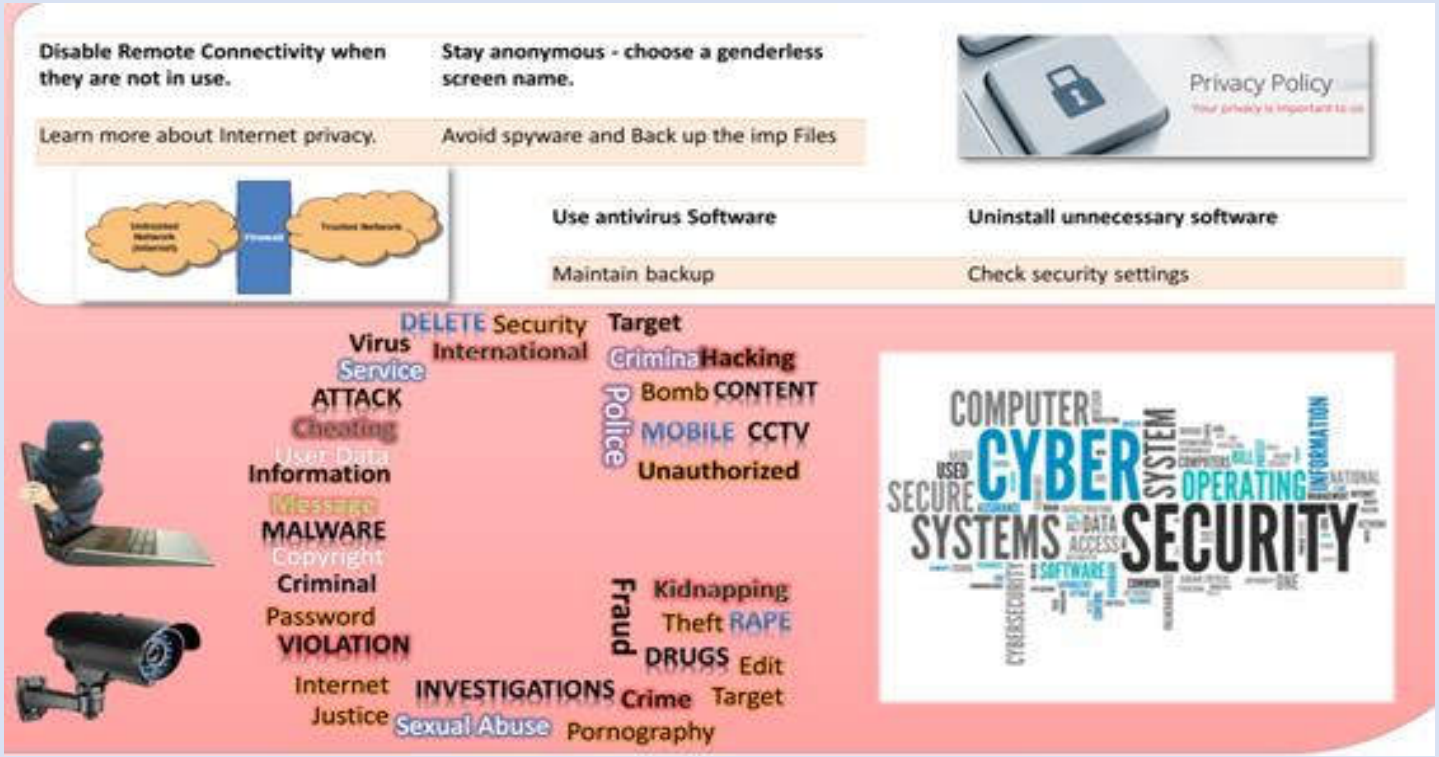
- Unwanted sexually explicit emails or other messages;
- Offensive advances in social media and other platforms;
- Threat of physical or sexual violence;
- Hate speech meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and/or other traits (such as sexual orientation or disability).




# Cyber Prevention for everyone

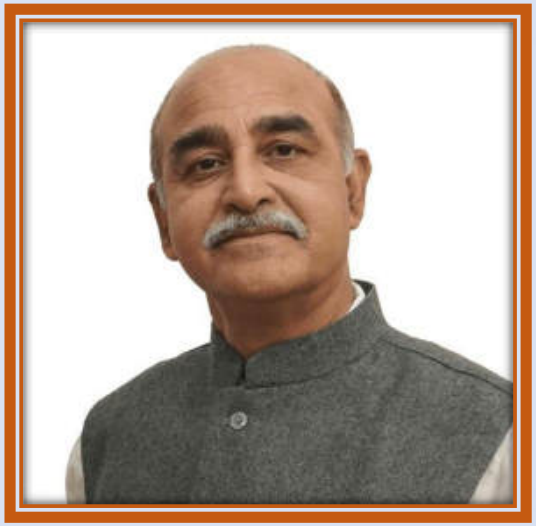
***Cyber Security*** is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, *security* includes both *cyber security* and physical *security*.

| | |
|---|---|
| 1) Physical Security | Protection of computer network / Internet of Things (IOT) from unauthorized access. |
| 2) Access Control | Using Firewalls allow only authorized communications between the internal and external network. |
| 3) Password | Password should be changed with regular interval of time and it should be alpha numeric and should be difficult to judge. Prevent the identification theft. |
| 4) Privacy Policy | Before submitting your name, e-mail, address, on a website look for the sites privacy policy. |
| 5) Finding weakness of network | Organization should work hard to discover security holes, bugs and weaknesses and report their findings as they are confirmed. |

# References


1. https://devgan.in/ipc/section/354D/
2. https://www.ecsbiztech.com/cyber-forensics/
3. https://www.coe.int/en/web/cyberviolence/types-of-cyberviolence
4. https://www.interpol.int/en/Crimes/Cybercrime
5. https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html
6. https://www.legalservicesindia.com/law/article/2266/6/Cyber-Crime-In-India
7. https://dfsl.maharashtra.gov.in/en/cyber-forensic#
8. APC Forensic Medicine and Toxicology by Dr. Anil Aggrawal
9. The Essentials of Forensic Medicine and Toxicology by Narayan Reddy
10. Review Of Forensic Medicine And toxicology by Gautam Biswas



## Message from Executive Director:

I heartily congratulate the Department of Forensic Medicine & Toxicology for bringing this informative newsletter. It will certainly be helpful for the community & medical students. My best wishes to the entire team…

Prof. Dr. (Col.) C.D.S. Katoch

## Message from Editors:

We hope you will find this piece of work interesting and informative. Our attempt through this newsletter is to spread awareness among the community, readers and medical students about cyber-crime. Your suggestions are always welcome.

Prof. (Dr.) Sanjay Gupta
Dr. Utsav Parekh