

## MOBILE RECHARGE SHOP

A Mobile Recharge Shop is a place where scamsters can gain access to your cellphone number because you have provided it to the recharge vendor. They will misuse your number to call or text you, exploit your ignorance or even emotionally manipulate you.

### IT Sections Applicable

#### **IPC Sections (to be applied to the Shop Keeper)**

- IPC Section 354A/BNS 75** - Sexual Harassment and punishment for Sexual Harassment
- IPC Section 354C/ BNS 77** - Voyeurism
- IPC Section 383/384/ BNS 308** - Extortion (IF ANY DEMAND)
- IPC Section 503/BNS 351** - Criminal Intimidation
- IPC Section 506/BN 351** - Punishment for Criminal Intimidation
- IPC Section 509/BNS 79** - Word, gesture or act intended to insult modesty of a woman

#### **IT Act:**

- IT Act Section 66E** - Punishment for violation of privacy

#### **Mobile Number Sale to Stalkers by Recharge Shop:**

#### **IPC Sections (to be applied to the Shop Keeper)**

- IPC Section 109/BNS 49** - Punishment for abetment
- IPC Section 114/BNS 54** - Abettor present when offence is committed
- IPC Section 120B/BNS 61** - Punishment for Criminal Conspiracy
- IPC Section 406/BNS 316** - Punishment for Criminal Breach of Trust

**Everything comes for a Charge and in case of Recharge, there's no Free Charge!**

## DEBIT CARD CLONING

Debit Card skimming happens when the PIN is revealed to another person. A scamster who knows the PIN and has possession of the card even for a short while can replicate the card with a skimming /schimming device and withdraw cash.

### IT Sections Applicable

#### **IT Act for cloning**

**Section 43:** This section deals with unauthorized access to computer systems, data breaches, and other computer-related offenses.

**IT Act Section 66** – Computer related offences

**IT Act Section 66C** – Punishment for Identity Theft

**IT Act Section 66D** – Punishment for cheating by personation using computer resource

#### **Money Transaction followed by cloning:**

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IPC Section 420/BNS 318** – Cheating

**IT Act Section 66D** – Punishment for cheating by personation by using computer resource.

**IT Act Section 72A** – This section deals with the punishment for disclosing personal information obtained in the course of providing services under the terms of lawful contract.

**IT Act Section 84A** – This section empowers the Central Government to prescribe modes or methods for encryption.

**Cloning may blow up your Earnings!**

## KEYLOGGER

It is a malicious program that may be installed on the victim's computer for recording computer user keystrokes to steal passwords and other sensitive information. With Keylogger a scamster will be able to collect login details and other matter saved in the computer and have them mailed to a designated email address.

### IT Sections Applicable

#### **Key logger installation: IT Act**

**IT Act Section 43** – Deals with unauthorized access, damage to computer systems, and data.

**IT Act Section 66** – Computer Related Offences

#### **Stealing personal information: IT Act**

**IT Act Section 66C** – Punishment for Identity Theft

#### **Creating fake profile & posting private conversation :**

**IT Act Section 66C** – Punishment for Identity Theft

**IT Act Section 66D** – Punishment for cheating by personation by using computer resources

**IT Act Section 67** – Punishment for publishing or transmitting obscene material in electronic form

**IT Act Section 67A** – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

**IT Act Section 67B** – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

**IT Act Section 72** – Breach of Confidentiality and Privacy

**IT Act Section 79** – Intermediary Liability Protection

#### **IPC Sections:**

**IPC Section 354A/BNS 75** – Sexual Harassment and punishment for Sexual Harassment

**If in hard copy, IPC Sections 292/BNS 294, 293/BNS 295  
294/BNS 296**

**Keylogger may empty your Coffers!**

## SMS SPOOFING

Spoofing is being able to send a message by hiding or changing or using a completely different sender ID. Typically, when you send an SMS, your handheld device sends the message with your phone number as the originator where in you as the sender cannot alter that number.

### IT Sections Applicable

#### **Act of hoax or trick or deceive a communication**

##### **IPC Section**

**IPC Section 465/BNS 336** – Making a false document (FORGERY)

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IT Act Section 43** – While not directly related to SMS

spoofing, this section deals with unauthorized access to computer systems, which could apply if someone gains unauthorized access to systems for the purpose of carrying out SMS spoofing.

**IT Act Section 43A and Section 72A:** These sections deal with the compensation for failure to protect data and confidentiality of information. If SMS spoofing leads to a breach of sensitive information, these sections might come into play.

**IT Act Section 66C** – This section deals with identity theft. If SMS spoofing is used to impersonate someone else and commit fraud or deceive others, it could be covered under this section.

**IT Act Section 66D** – Punishment for cheating by personation by using computer resource

**IT Act Section 66E** – This section addresses violations of privacy and the capturing, publishing, or transmitting of images of a private area of any person without their consent. If SMS spoofing is used to invade someone's privacy in this manner, this section could apply.

**SMS are Spoofed by Cyber Crooks!**

## CALL SPOOFING

Call spoofing happens through apps that enable a person with criminal intent to change his number and voice to impersonate another to defraud.

### IT Sections Applicable

#### **Act of hoax or trick or deceive a communication**

##### **IPC Section**

**IPC Section 465/BNS 336** – Making a false document( FORGERY)

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IT Act Section 66C – Identity Theft** : This section of the Information Technology Act deals with identity theft, which includes dishonestly or fraudulently making use of the electronic signature, password or any other unique identification feature of any other person. Call spoofing can fall under the ambit of this section if it involves stealing someone's unique identification feature for wrongful gain.

**Additionally, IT Act Section 66D** – Cheating by Personation using Computer Resource can also be applied. This section addresses cheating by personation through the use of a computer resource. If call spoofing is done with the intention to cheat or deceive someone, it could potentially fall under this section.

**Call Spoofing is always with criminal intent!**

## RANSOMWARE

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data. Users are shown instructions as to how to pay a fee to get the decryption key. The costs can range from a few hundred rupees to thousands, payable to cyber criminals in bitcoin.

### IT Sections Applicable

#### **Unauthorised access, Denial, Encryption :**

**IT Act Section 43** – This section deals with unauthorized access, damage to computer systems, and data breaches.

**IT Act Section 66** – Computer related offences

**Section 66C** – This section deals with identity theft.

**Section 66D** – This section deals with cheating by impersonation using a computer resource.

#### **Demand without payment :**

**IPC Section 384/BNS 308** – Extortion

**IT Act Section 386/BNS 308** – This section deals with extortion by a putting person in fear of death or grievous hurt.

**IPC Section 511/BNS 62** – Punishment for attempting to commit offence punishable with imprisonment for life or other imprisonment

#### **Demand & payment :**

**IPC Section 384/BNS 308** – Extortion

**Sensitize your Hardware and Software to avoid Ransomware!**

## CYBER STALKING

Cyber stalking is the use of the Internet or other electronic means to stalk or harass another by misusing information uploaded on social networking sites.

### IT Sections Applicable

**Section 66A** – This section previously dealt with the offense of sending offensive messages through communication services. However, it was struck down by the Supreme Court of India in 2015 on grounds of being vague and overbroad, and violating the right to free speech.

#### **Offline:**

**IPC Section 354 D/BNS 78** – Stalking

#### **Online :**

**IPC Section 354 D/BNS 78** – This section was introduced through the Information Technology (Amendment) Act, 2013, and specifically deals with the offense of cyber stalking. It states that any person who monitors these by a woman of the internet, email, or any other form of electronic communication, commits the offense of cyber stalking. It also criminalizes actions that cause the woman to fear for her safety or the safety of her relatives. Conviction under this section can result in imprisonment for a term which may extend to three years and a fine.

**Cyber stalking means  
someone is keeping an eye on you remotely!**

## PICTURE MORPHING

Morphing the face of a person to the body of another and publishing it to blackmail or otherwise intimidate the person is one of the ways by which people who upload photos on social networking sites can be exploited.

### IT Sections Applicable

#### **IPC Sections**

**IPC Section 292/BNS 294** – Sale etc of Obscene books etc  
(if in hardcopy)

**IPC Section 465/BNS 336** – Morphing photographs and creating a false electronic record

**IPC Section 469/BNS 336** – Making false electronic document for causing defamation

**IPC Section 507/BNS 351** – Criminal Intimidation by an Anonymous communication

**IPC Section 509/BNS 79** – Word, gesture or act intended to insult modesty of a woman

#### **IT Act**

**Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

**Section 66E** – Punishment for Violation of Privacy

**Section 67** – Punishment for publishing or transmitting obscene material in electronic form

**Section 67A** – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

**Section 67B** – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

**Section 72** – Penalty for Breach of Confidentiality and Privacy

**For publishing photos containing indecent representation of women:**  
Section 4 R/W Section 6 of Indecent Representation of Women's Act, 1986

**Morphing is used for Defaming!**



## PROFILE HACKING

Profile Hacking happens when your email or social networking profile is accessed by a probable stalker who then compromises it.

### IT Sections Applicable

#### IT Act

- Section. 43** – Unauthorized access to computer systems, networks, data.
- Section 66** – Computer related offences
- Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using password)
- Section. 66D** – Impersonation cheating through computer resources.

#### IPC Section. 379/BNS 303 & 380/BNS 305 :

Theft of data or credentials.

#### IPC Section. 463/BNS 336, 464/BNS 335, 468/BNS 336 :

Forgery of electronic records for fraud.

#### IPC Section. 507/BNS 351 :

Criminal intimidation through hacking.

**Profile Hacking means Security is Lacking!**

## ONLINE GAMES

Girls who are vulnerable to loneliness, low self-esteem and clinical depression can fall prey to dangerous online games that may become addictive and further harm them. Some dangerous online games like the blue whale challenge even end in the victim ending her life. This is a personal as well as social challenge for the others around.

### IT Sections Applicable

#### **Information Technology Act, 2000:**

**Section 43** – This section deals with unauthorized access to computer systems, computer networks, or data. It covers actions such as hacking, introducing viruses, and damaging computer systems.

**Section 66** – This section deals with computer-related offenses, including hacking, identity theft, and other forms of cyber crime

**Section 67A** – This section deals with the punishment for publishing or transmitting sexually explicit content in electronic form.

**Section 67B** – This section deals with the punishment for publishing or transmitting material depicting children in sexually explicit acts.

**Section 79** – This section provides safe harbor to intermediaries, including online platforms and game hosting services, from liability for third-party content. However, they are required to adhere to certain conditions, including taking down illegal content upon receiving notice.

#### **IPC Sections**

**IPC Section 299/BNS 100** – Culpable homicide

**IPC Section 305/BNS 107** – Abetment of suicide of Child or Insane Person

**IPC Section 306/BNS 108** – Abetment of suicide

**IPC Section 321/BNS 115** – Voluntarily causing hurt

**IPC Section 335/BNS 122** – Voluntarily causing grievous hurt on provocation

**IPC Section 336/BNS 125** – Act endangering life or personal safety of others

**Before it becomes a game changer of your child's Future, keep track what they do on their personal Computers (laptops, iPads, mobile phones, tabs, desktop etc).**

## JOB CALL LETTER

Websites offering jobs need to be checked for veracity and authenticity. Mails need to be double-checked and verified before one responds and acts on instructions provided, especially if one is asked to put in a personal appearance.

### IT Sections Applicable

#### **Fake account / ID: IT Act**

**Section 43A** – Compensation for failure to protect data: This section deals with the liability of a body corporate in case of a breach of sensitive personal data due to negligence in implementing and maintaining reasonable security practices and procedures.

**Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

**Section 66D** – Punishment for cheating by personation by using computer resource

**Section 72** – Breach of confidentiality and privacy: This section deals with the punishment for breach of confidentiality and privacy.

**Section 72A** – Punishment for disclosure of information in breach of lawful contract: This section pertains to the punishment for revealing information in breach of a lawful contract.

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IPC Section 420/BNS 318** – Cheating

**IPC Section 465/BNS 336** – Making a false document (DEFINITION SECTION)

**IPC Section 468/BNS 336** – Forgery for cheating

**IPC Section 471/ BNS 340** – Using forged document as genuine

**IPC Section 474/BNS 339** – Procession of forged document

**IPC Section 120B/BNS 61** – Punishment for Criminal Conspiracy

**IPC Section 34/BNS 3(5)** – Acts done by several persons in furtherance of Common Intention

#### **Abatement for offence**

**a. On the spot :** IPC Section 114/BNS 54 – Abettor present when offence is committed

**b. Remotely:** IPC Section 109/BNS 49 – Punishment for abetment

**Such fake call letters may see you out of your existing job sooner or later!**

## DEEPPAKES

Deepfake is a technique that is used to combine and superimpose new images and videos onto source images or videos. It is used to create videos where the voice or face of another is superimposed on the original in such a way that the viewer or listener cannot distinguish or doubt the veracity of it.

### IT Sections Applicable

**Fake account / ID:**

**IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)**

**Impersonation for cheating :**

**IT Act Section 66D – Punishment for cheating by personation by using computer resource.**

**ITA Section 43A and Section 72A of the Information Technology Act, 2000 – Compensation for Failure to Protect Data and Privacy:** These sections deal with the compensation payable to an individual whose personal data and information have been negligently disclosed, which could be applicable in cases where deepfakes lead to privacy breaches.

**IPC Section 419/BNS 319 – Punishment for cheating by personation**

**IPC Section 420/BNS 318 – Cheating**

**Publishing online:**

**IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form**

**IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form**

**IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO**

**IPC**

**Section 354A/BNS 75 – Sexual Harassment and punishment for Sexual Harassment**

**Section 465/BNS 336 – Making a false document**

**Section 499/BNS 356 – Defamation**

**Section 500/BNS 356 – Punishment for Defamation**

**Section 507/BNS 351 – Criminal Intimidation by an Anonymous communication**

**SEC 509/BNS 79 – Insulting modesty of women**

**Stalking: IPC Section 354 D/BNS 78 – Stalking Offline**

**: IPC Section 354 D/BNS 78 – Stalking Online**

**IPC Section 120-B/BNS 61 – Punishment for Criminal Conspiracy**

**IPC Section 34/BNS 3(5) – Acts done by several persons in furtherance of Common Intention**

**Abatement for offence:**

**a. On the spot: IPC Section 114/BNS 54 – Abettor present when offence is committed**

**b. Remotely: IPC Section 109/BNS 49 – Punishment for abetment**

**Deep Fakes are not noticeable easily and hence have High Stakes!**

## DATING WEBSITE

Females can be emotionally manipulated by smooth talkers on dating sites. Any private pictures or texts that they send across to probable dating companions on such sites are fair game for unscrupulous persons who can then blackmail them.

### IT Sections Applicable

**ITA Section 43A** – This section deals with the compensation for failure to protect data and is relevant for data breaches.

**IT Act Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

**IT Act Section 66D** – Punishment for cheating by personation by using computer resource.

**Section 72A:** This section penalizes the disclosure of personal information without consent.

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IPC Section 420/BNS 318** – Cheating

**IPC Section 354A/BNS 75** – Sexual Harassment and punishment for Sexual Harassment

**IPC Section 354C/BNS 77** – Voyeurism

**IPC Section 354D/BNS 78** – Deals with stalking.

**Stalking : Offline – IPC Section 354 D/BNS 78 – Stalking**

**Online – IPC Section 354 D/BNS 78 – Stalking**

**Publishing online:**

**IT Act Section 67** – Punishment for publishing or transmitting obscene material in electronic form

**IT Act Section 67A** – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

**IT Act Section 67B** – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form  
Et sections of POCSO

**IPC Section 507/BNS 351** – Criminal Intimidation by an Anonymous communication

**IPC Section 509/BNS 79** – Word, gesture or act intended to insult modesty of a woman

**IPC Section 465/BNS 336** – Making a false document

**Looking out for a Date, be careful that you don't get Check-Mate!**

## CAMERA HACKING ■

Camera hacking happens when photographs of a person are taken without consent, through malware that got downloaded with an attachment. Phones with no camera guard can be exploited for such criminal activities. ■

### IT Sections Applicable

#### **Hacking–**

**IT Act Section 43** – Penalty for unauthorized access to computer systems, data disruption, and theft.

**IT Act Section 66** – Computer related offences

**Section 66B** – Punishment for dishonestly receiving stolen computer resources or communication devices.

#### **Capturing photograph/video:**

**IPC Section 354C/BNS 77** – Voyeurism

**IT Act Section 66E** – Punishment for violation of privacy

#### **Creating Fake ID in social media**

**IT Act Section 66D** – Punishment for cheating by personation by using computer resource

**IPC Section 419/BNS 319** – Punishment for cheating by personation

#### **Online Sexual harassment to a woman**

**IPC Section 354A/BNS 75** – Sexual Harassment and punishment for Sexual Harassment.

**IPC Section 354C/BNS 77** – Voyeurism (capturing or transmitting images of private parts without consent).

**Stalking : Offline** : **IPC Section 354D/BNS 78** – Stalking

**Online** : **IPC Section 354D/BNS 78** – Stalking

#### **Publishing online**

**IT Act Section 66F** – Cyber Terrorism under the IT Act

**IT Act Section 67** – Punishment for publishing or transmitting obscene material in electronic form

**IT Act Section 67A** – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

**IT Act Section 67B** – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO.

**IT Act Section 72** – Breach of Confidentiality and Privacy under the IT Act

**IPC Section 507/BNS 351(4)** – Criminal Intimidation by an Anonymous communication

**IPC Section 509/BNS 79** – Word, gesture or act intended to insult modesty of a woman

**Think before taking your cell phones while using the restroom.  
Your privacy may have no room to rest!**

## SOCIAL TROLLING

Social Trolling is posting inflammatory messages or visuals about a person or organisation in an online community with the sole intention of causing humiliation or nuisance to that person.

### IT Sections Applicable

**IPC Section 507/BNS 351** – Criminal Intimidation by an Anonymous communication

**IPC Section 509/BNS 79** – Word, gesture or act intended to insult modesty of a woman

#### **Stalking:**

**Offline: IPC Section 354D/BNS 78** – Stalking

**Online : IPC Section 354D/BNS 78** – Stalking

**IT Act Section 66A** – Punishment for sending offensive messages through communication service, etc.

**IT Act Section 66C** – Punishment for identity theft.

**IT Act Section 67A** – Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

**IT Act Section 67B** – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

**Are you Trolling, the law may be soon following!**

## PONZI SCHEME

A Ponzi scheme is a fraudulent investing scam promising high rates of return with little risk to investors. Victims of such schemes are vulnerable to hackers with malicious intent and fall prey to their promises of recovery of their losses.

### IT Sections Applicable

Sections 3, 4, 5, 6 of Prize Chits and Money Circulation Schemes (Banning) Act, 1978

Also look up at State Acts eg

Section 9 of the Karnataka Protection of Interest of Depositors In Financial Establishments Act, 2004

Section 3, 4 of Maharashtra Protection of Interest of Depositors In Financial Establishments Act, 1999 etc.

**SEBI Act, 1992 – Section 11B:** This empowers SEBI to counter fraudulent practices in securities trading, including Ponzi schemes.

**Companies Act, 2013 – Section 447:** It penalizes fraud, encompassing Ponzi schemes, with imprisonment and fines.

**IPC Section 120B/BNS 61** – Punishment for Criminal Conspiracy

**IPC Section 406/BNS 316** – Punishment for Criminal Breach of Trust

**IPC Section 420/BNS 318** – Cheating

**IPC Section 34/BNS 3(5)** – Acts done by several persons in furtherance of Common Intention

**Investing in Ponzi schemes may make you run out of all other Schemes of life!**



## FAKE MATRIMONIAL PROFILE

A fraudster may have registered on a matrimonial site with a fake profile. The details and profile pic may not be his. He can dupe a naive girl who falls for his practised charm and believes in the authenticity of supportive material that he provides to back up his identity.

### IT Sections Applicable

**IT Act Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

**IT Act Section 66D** – Punishment for cheating by personation by using computer resource

**IT Act Section 66E** – Punishment for violation of privacy.

- |                                   |                                                          |
|-----------------------------------|----------------------------------------------------------|
| <b>IPC Section 415/BNS 318</b>    | - Punishment for cheating.                               |
| <b>IPC Section 419/BNS 319</b>    | - Punishment for cheating by personation                 |
| <b>IPC Section 420/BNS 318</b>    | - Cheating                                               |
| <b>IPC Section 464/BNS 335</b>    | - Making a false document.                               |
| <b>IPC Section 465/BNS 336(2)</b> | - punishment for forgery                                 |
| <b>IPC Section 468/BNS 336(3)</b> | - Forgery for purpose of cheating.                       |
| <b>IPC Section 471/BNS 340</b>    | - Using as genuine a forged document.                    |
| <b>IPC Section 507/BNS 351</b>    | - Criminal Intimidation by an<br>Anonymous communication |

**Marriages are made in Heaven but in the virtual world you end up paying the cost of messing with Heavenly Affairs!**

## MOBILE REPAIR SHOP

Pictures and videos stored in the phone's gallery can be accessed by any person once the phone is in his possession. A mobile repair shop may have a criminal who accesses private pictures or other data and uploads them on shady sites to make them viral. He may also use them for blackmailing.

### IT Sections Applicable

**IT Act Section 43A** - This section deals with compensation for failure to protect sensitive personal data.

**IT Act Section 66** - Computer Related Offences

**IT Act Section 66C** - Prohibits identity theft, which includes impersonating someone with the intent to cause wrongful loss.

**IT Act Section 66D** - Deals with cheating by impersonation using computer resources.

**IT Act Section 72A** - It criminalizes the disclosure of personal information without consent, intending to cause wrongful loss or gain

**IPC Section 406/BNS 316** - Punishment for Criminal Breach of Trust

#### **Publishing online**

**IT Act Section 67** - Punishment for publishing or transmitting obscene material in electronic form

**IT Act Section 67A** - Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

**IT Act Section 67B** - Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

**IPC Section 506/BNS 351** - Punishment for Criminal Intimidation

**IPC Section 507/BNS 351** - Criminal Intimidation by an Anonymous communication

**IPC Section 509/BNS 79** - Word, gesture or act intended to insult modesty of a woman

**Indian Copyright Act, 1957 - Section 63B: Online Copyright Infringement**  
**Section 63B** deals with the offense of knowingly circumventing technological measures to infringe copyright.

**If caution not adhered at such Shops, get ready to take big Hops!**

## FAKE REVIEWS

A website may dupe customers by putting up fake reviews of products. They plant glowing reviews and pay for perfect ratings that attract customers, especially backed by discounted prices. These products from dubious sites may cause untold harm if used.

### IT Sections Applicable

**IPC Section 406/BNS 316** – Punishment for Criminal Breach of Trust

**IPC Section 420/BMS 318** – Cheating

**IT Act Section 43(a)** – Compensation for Damage to Computer, Computer System, etc. (IT Section 66C – Punishment for Identity Theft (IT Act, 2000))

**IT Act Section 66D** – Punishment for Cheating by Personation (IT Act, 2000)

**IT Act Section 66F** – Punishment for Cyber Terrorism (IT Act, 2000)

**Fake Reviews may give you wrong Overviews!**

## FAKE PROFILE WITH SEXTORTION

Public changing rooms may have strategically placed cameras that capture pics of the users, naturally with criminal intent. These pics can then be uploaded on a duplicate social media account with the intention of extortion.

### IT Sections Applicable

#### **Capturing photograph/video:**

**IT Act Section 43** – Unauthorized access to computer systems, data, or information.

**IT Act Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

**IT Act Section 66D** – Punishment for cheating by personation by using computer resource

**Section 66E** – Violation of privacy.

**IPC Section 415/BNS 318** – Cheating.

**IPC Section 416/BNS 319** – Cheating by personation.

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IPC Section 354A/BNS 75** – Sexual Harassment and punishment for Sexual

**IPC Section 354C/BNS 77** – Voyeurism

**IPC Section 354D/BNS 78** – Stalking.

**IPC Section 503/BNS 351** – Criminal intimidation.

**IPC Section 507/BNS 351** – Criminal Intimidation by an Anonymous communication

#### **Publishing online**

**IT Act Section 67** – Punishment for publishing or transmitting obscene material in electronic form

**IT Act Section 67A** – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

**IT Act Section 67B** – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

**IPC Section 509/BNS 79** – Word, gesture or act intended to insult modesty of a woman

**A Fake Profile can cause unimaginable consequences!**

## CYBER VULTURES

Cyber-vultures are a merciless breed of hackers who like to feast on consumers and businesses suffering from any type of attack. They use this scenario as an opportunity to trick them and swindle more money.

### IT Sections Applicable

**IT Act Section 66** – Computer related offences

**IT Act Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

**IT Act Section 67** – Punishment for publishing or transmitting obscene material in electronic form.

**IT Act Section 67A** – Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

### **Impersonation as financial company:**

**IT Act Section 66D** – Punishment for cheating by personation by using computer resource

### **Fetching personal/ Banking/wallet details:**

**IT Act Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature/password/electronic signature)

**IPC Section 420/BMS 318** – Cheating

**Vultures live on dead bodies, cyber vultures live on people who have already lost their money (who are dead financially).**

## APP TRAPS

The internet could come with a hidden cost. One of these is preloaded apps that harvest users' data without their knowledge. These apps ask for permission to access files and once given, they may use videos, photos and storage media not only to be mined by marketers but also for other nefarious purposes.

### IT Sections Applicable

**IPC Section 406/BNS 316** – Punishment for Criminal Breach of Trust

**IPC Section 420/BMS 318** – Cheating

#### **Information Technology Act, 2000 (IT Act):**

**a. IT Act Section 43A** – This section deals with the compensation for failure to protect data. Organizations handling sensitive personal data are required to implement reasonable security practices to protect such data. If they fail to do so and a person suffers harm as a result, the organization could be liable to pay compensation.

**b. IT Act Section 66** – This section deals with computer-related offenses, including unauthorized access, data theft, and damage to computer systems.

**These traps give you a silent rap and take away your sensitive personal data.**

## JUICE JACKING

Juice Jacking is a type of cyber attack involving a charging port that doubles as a data connection, typically over USB. This often involves either installing malware or copying sensitive data from a smart phone or other computer devices. Charging ports at public places are prime areas for juice jacking.

### IT Sections Applicable

- IT Act Section 43** – This section deals with unauthorized access to computer systems, computer networks, or resources.
- IT Act Section 66** – Computer Related Offences
- IT Act Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature/password/electronic signature)
- IT Act Section 66D** – This section pertains to cheating by personation using a computer resource.
- IT Act Section 66E** – This section deals with violation of privacy.
- IT Act Section 72** – This section deals with the breach of confidentiality and privacy of information.

**Data Theft** – **IPC Section 379/BNS 303**

**You may end up giving your data by way of Lottery to the fraudster as against the life of your Battery.**

## WIFI HACKING

Wifi hacking is essentially cracking the security protocols in a wireless network, granting full access for the hacker to view, store, download, or abuse the wireless network. Weak passwords to wifi networks may enable a hacker to log into the net through the wifi connection in the vicinity.

### IT Sections Applicable

**IT Act Section 66** – Computer Related Offences

**IT Act Section 66B** – Punishment for dishonestly receiving stolen computer resource or communication device

**IT Act Section 66C** – Identity Theft

**IT Act Section 72** – Breach of Confidentiality and Privacy

**Wrongful gain, wrongful loss of internet data:**

**IPC Section 420/BNS 318** – Cheating

**Mischief by internet utility:**

**IPC Section 425/BNS 324/426/BNS 324** – Mischief

**Publishing online**

**IT Act Section 67** – Punishment for publishing or transmitting obscene material in electronic form

**IT Act Section 67A** – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

**IT Act Section 67B** – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

Other provisions of Narcotic Drugs and Psychotropic Substances Act, 1985.

**To live a highfy virtual life, better secure your Wi-Fi!**



## ONLINE RADICALIZATION

Young, vulnerable individuals can fall prey to terrorists' propaganda while spending time online and browsing the net. The targets of such extremists are individuals or groups of people who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

### IT Sections Applicable

- IT Act Section 66F** – Punishment for Cyber Terrorism
- IPC Section 120-B/BNS 61** – Punishment of Criminal Conspiracy
- IPC Section 121/BNS 147** – Waging or attempting to wage war, or abetting waging of war, against the Government of India
- IPC Section 121A/BNS 148** – Conspiracy to commit offences punishable under Section 121A
- IPC Section 122/BNS 149** – Collecting arms, etc., with intention of waging war against the Government of India

**Don't get Radicalized, rather be Rationalized!**

## HONEY TRAP

Honey trapping is an investigative practice that uses romantic or intimate relationships for an interpersonal, political or monetary purpose to obtain sensitive information. In today's cyber world, "Honey Trap" has gained a new dimension on social media platforms like Facebook, Twitter etc to trap targets by blackmailing them.

### IT Sections Applicable

#### **Capturing Picture/Video Over Online:**

**IPC Section 354C/BNS 77** - Voyeurism

**IPC Section 509/BNS 79** - Word, gesture or act intended to insult modesty of a woman

**IT Act Section 66E** - Punishment for violation of privacy

**IT Act Section 67** - Punishment for publishing or transmitting obscene material in electronic form

**IT Act Section 67A** - Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

**IT Act Section 67B** - Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

#### **Demand for ransom (attempt):**

**IPC Section 385/BNS 308** - Putting person in fear of injury in order to commit extortion

**IPC Section 511/BNS 62** - Punishment for attempting to commit offence punishable with imprisonment for life or other imprisonment

**With AI, it becomes almost difficult if not impossible to make out the real from surreal.**

## QR CODE SCAM

A QR (Quick Response) code is nothing more than a two-dimensional barcode. This type of code was designed to be read by robots that keep track of produced items in a factory. As a QR code takes up a lot less space than a legacy barcode, its usage soon spread and Hackers took it to their advantage! QR codes are easy to generate and hard to tell apart from one another. To most human eyes, they all look the same.

### IT Sections Applicable

**IPC Section 406/BNS 316** – Punishment for Criminal Breach of Trust

**IPC Section 420/BMS 318** – Cheating

#### **Unauthorised Access by installing malware in the background:**

- |                           |                             |
|---------------------------|-----------------------------|
| <b>IT Act Section 43</b>  | – Unauthorized Access       |
| <b>IT Act Section 66</b>  | – Computer related offences |
| <b>IT Act Section 66C</b> | – Identity Theft            |
| <b>IT Act Section 66D</b> | – Cheating by Personation   |
| <b>IT Act Section 66E</b> | – Privacy Violation         |

**Your money may be at stake because the codes or apps downloaded by you can be fake.**

## RFID CLONING

Radio frequency identification, or RFID often abbreviated Radio Frequency Identification is method for automatic identification of objects, where the object IDs read or write data using radio waves. Each chip contains an identifier stored inside, with unique number and antenna. Most of these cards can be cloned, easily!

### IT Sections Applicable

**IT Act Section 66** – Computer Related Offences

**Stealing RFID data / RFID Cloning:**

**IT Act Section 66C** – Punishment for Identity Theft  
(dishonestly or fraudulently using a unique identification feature/  
password/electronic signature)

**Retaining stolen data & Selling Credit Card Details:**

**IT Act Section 66B** – punishment for dishonestly receiving  
stolen computer resource or communication device

**IPC Section 420/BNS 318** – Cheating

**Creating Replica of Digital ID & accessing server by impersonation:**

**IT Act Section 66** – Computer Related Offences

**IT Act Section 66C** – Punishment for Identity Theft  
(dishonestly or fraudulently using a unique identification feature)

**IT Act Section 66D** – Punishment for cheating by personation  
by using computer resource

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**Use technology only if you can imbibe Cyber Hygiene in your Genes.**

## DRONE SURVEILLANCE

In aviation and in space, a drone refers to an unpiloted aircraft or spacecraft. Drones can be equipped with various types of surveillance equipment that can collect high definition video and still images day and night. Drones can be equipped with technology allowing them to intercept cell phone calls, determine GPS locations, and gather license plate information.

### IT Sections Applicable

Following/Stalking/Capturing any PRIVATE AREA pic /video of a women by DRONE without her consent:

**IPC Section 354A/BNS 75** – Sexual Harassment and punishment for Sexual Harassment

**IPC Section 354C/BNS 77** – Voyeurism

**IPC Section 354D/BNS 78** – Stalking

**IPC Section 509/BNS 79** – Word, gesture or act intended to insult modesty of a woman

**IT Act Section 66E** – Punishment for violation of privacy

**Unauthorised access to WI FI by DRONE:**

**IT Act Section 66** – Computer Related Offences

**Stealing personal information via WI FI Cracker:**

**IT Act Section 66C** – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

**Dropping hazardous materials to house via DRONE:**

**IPC Section 436/BNS 326** – Mischief by fire or explosive substance with intent to destroy house, etc.

**You are profiled day in and day out without doubt.**

## SEARCH ENGINE RESULTS SCAM

A hacker can create a legitimate-looking website and get it indexed by various search engines, making it appear in search results based on the keywords you type. This way, misleading results, fake help line numbers etc can be displayed, making the user believe them and fall prey to this Search Engine Optimization (SEO) scam.

### IT Sections Applicable

**IT Act Section 66** – Computer Related Offences

**Replacing Original Contact Details by Fraudster Details:**

**IT Act Section 66C** – Punishment for Identity Theft  
(dishonestly or fraudulently using a unique identification feature)

**IT Act Section 66D** – Punishment for cheating by personation  
by using computer resource

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IPC Section 420/BNS 318** – Cheating

**IPC Section 465/BNS 336** – Making a false document

**IPC Section 468/BNS 336** – Forgery for the purpose of cheating

**Fake numbers of customer care may put you under intensive care.**

## IDN HOMOGRAPH ATTACK

An IDN homograph attack is similar to another type of domain name spoofing known as typo squatting. Both techniques attempt to deceive users by using a new domain name that's similar to an established name, although they exploit different types of similarities.

### IT Sections Applicable

**IT Act Section 66** – Computer related offences

**IT Act Section 66C** – Punishment for Identity Theft

**IT Act Section 66D** – Punishment for cheating by personation using a computer resource

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IPC Section 420/BNS 318** – Cheating

**Crackers replacing Letters & Characters to commit frauds.**

## SCRATCH CARD SCAM

A user receives a message with a link to a third-party website with a promise of winning guaranteed money. When the user clicks on the link, it redirects to a website with a scratch card mimicking the design of popular Pay Wallets scratch card.

### IT Sections Applicable

**IT Act Section 66** – Computer related offences

**IT Act Section 66C** – Punishment for Identity Theft

**IT Act Section 66D** – Punishment for cheating by personation using a computer resource

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IPC Section 420/BNS 318** – Cheating

**Sharing sensitive Credentials will bring about losses that would be Substantial**



## SIM SWAP

A SIM swap scam (also known as port-out scam, SIM splitting, Smishing and sim jacking, SIM swapping) is a type of account takeover fraud. The fraud exploits a mobile phone service provider's ability to seamlessly port a telephone number to a device containing a different SIM. This feature is normally used when a customer has lost or had their phone stolen, or is switching service to a new phone.

### IT Sections Applicable

**IT Act Section 66** – Computer related offences

**IT Act Section 66C** – Punishment for Identity Theft

**IT Act Section 66D** – Punishment for cheating by personation using a computer resource

**IPC Section 419/BNS 319** – Punishment for cheating by personation

**IPC Section 420/BNS 318** – Cheating

**Swapping of Sim could lead you to a situation thats Dim**

## CRYPTO JACKING

It is a type of cyber attack in which a hacker co-opts a target's computing power to illicitly mine crypto currency on the hacker's behalf. Crypto jacking can target individual consumers, massive institutions, and even industrial control systems. It slows down infected computers, as the mining process takes priority over other legitimate activities.

### IT Sections Applicable

- |                                |                                                                    |
|--------------------------------|--------------------------------------------------------------------|
| <b>IT Act Section 66</b>       | - Computer related offences                                        |
| <b>IT Act Section 66C</b>      | - Punishment for Identity Theft                                    |
| <b>IT Act Section 66D</b>      | - Punishment for cheating by personation using a computer resource |
| <b>IPC Section 419/BNS 319</b> | - Punishment for cheating by personation                           |
| <b>IPC Section 420/BNS 318</b> | - Cheating                                                         |
- Section of Prevention of Money Laundering Act, 2002 (PMLA), may apply as per the facts of the case.**

**Crypto jacking helps hackers in Money Making**

## VIDEO CONFERENCE SCAM

There has been a mass adaptation of online platforms to conduct meetings, online classes, conferences without giving much consideration to the security settings of these platforms. This has paved the way for cyber criminals to take advantage of loopholes for malicious purposes.

### IT Sections Applicable

- |                           |                                                                |
|---------------------------|----------------------------------------------------------------|
| <b>IT Act Section 66</b>  | - Computer related offences                                    |
| <b>IT Act Section 66C</b> | - Punishment for Identity                                      |
| <b>IT Act Section 67</b>  | - Publishing or transmitting obscene content                   |
| <b>IT Act Section 67A</b> | - Publishing or transmitting sexually explicit acts or conduct |

### **Theft**

- |                                |                                                                                                   |
|--------------------------------|---------------------------------------------------------------------------------------------------|
| <b>IT Act Section 66D</b>      | - Punishment for cheating by personation using a computer resource (as per the facts of the case) |
| <b>IPC Section 419/BNS 319</b> | - Punishment for cheating by personation                                                          |
| <b>IPC Section 420/BNS 318</b> | - Cheating (as per the facts of the case)                                                         |

**Inference of who's attending such virtual Conference needs to made**

## KIDS MOBILE PHONE

Children are using devices at a younger age and it's a tricky situation for most parents since they do not want their child to come across adult, abusive, or violent content on the internet. Thus, it's important to consider setting controls on the devices they use. Responsible mobile phone use is about managing costs, sticking to family rules, keeping phones safe and being respectful.

### IT Sections Applicable

#### **If Gambling is involved:**

The acts may attract Provisions of **IT Act Section 69A** for blocking illegal gambling websites.

The Public Gambling Act, 1867.

The Foreign Exchange Management Act, 1999 (FEMA).

The Lotteries Regulation Act of 1998.

A few States have made provisions for laws on Gambling.

#### **Exceptions:**

1. Horse racing is legal in India
2. Lottery system (in few States)
3. The Public Gambling Act of 1867 exempts skill-based games from the definition of gambling.

**Online games may bring about losses, disrepute and shame**

## SMART HOMES

Smart-home devices hold a treasure trove of personal information, from your birth date to credit card details, that cyber criminals can steal via hacking if the devices lack robust protections to thwart attacks. They can then use the stolen data to launch targeted attacks to rope you into shady deals.

### IT Sections Applicable

Digital outreach may lead to Privacy Breach

**IPC Section 354/BNS 74** – Sexual harassment

**IPC Section 354C/BNS 77** – Voyeurism

**IPC Section 509/BNS 79** – Outraging modesty of women

**IT Act Section 66** – Computer related offences

**IT Act Section 66E** – Punishment for violation of privacy

Digital outreach may lead to Privacy Breach

## MICRO LOANS

Fly-by-night micro lending illegal app-based financiers are thriving. These moneylenders target younger customers who look for quick loans for consumption purposes. Those failing to pay up will have their photos shared in their family and workplace social media groups, a tactic that has driven many to desperation.

### IT Sections Applicable

<b>IPC Section 420/BNS 318</b>	- Cheating
<b>IPC Section 503/BNS 351/ 506/BNS 351</b>	- Criminal Intimidation
<b>IPC Section 383/BNS 308</b>	- Extortion
<b>IPC Section 306/BNS 108</b>	- Abetment of Suicide
<b>IPC Section 499/BNS 356 / 500/BNS 356</b>	- Defamation
<b>IPC Section 120B/BNS 61</b>	- Criminal Conspiracy
<b>IPC Section 34/BMS 3(5)</b>	- Common Intention

Sections of Reserve Bank of India Act, 1934  
(as per the facts of the case)

**App based micro loans are Unsecured and the borrower becomes Insecure**

## BLUE SNARFING

It is a device hack performed when a wireless, Bluetooth-enabled device is in discoverable mode. Blue snarfing allows hackers to remotely access Bluetooth device data, such as a user's calendar, contact list, emails and text messages. This attack is perpetrated without the victim's knowledge.

### IT Sections Applicable

- |                                |                                                                                                   |
|--------------------------------|---------------------------------------------------------------------------------------------------|
| <b>IT Act Section 66</b>       | - Computer related offences                                                                       |
| <b>IT Act Section 66C</b>      | - Punishment for Identity Theft                                                                   |
| <b>IT Act Section 66D</b>      | - Punishment for cheating by personation using a computer resource (as per the facts of the case) |
| <b>IPC Section 419/BNS 319</b> | - Punishment for cheating by personation                                                          |
| <b>IPC Section 420/BNS 318</b> | - Cheating (as per the facts of the case)                                                         |

**Hacker may use your Bluetooth to route your information and cause you blues**

## STOLEN PHONE

A stolen phone can leave you feeling helpless and scrambling. Mobile phones and the data they hold are very valuable to thieves. And for similar reasons – they hold so much important personal information of real and sentimental value – a theft can be a huge loss for the owner.

### IT Sections Applicable

#### **IPC Section 378/BNS 303/ 379/BNS 303 – Theft**

This section deals with theft and covers the unlawful taking of movable property, including stolen phones.

#### **IPC Section 406/BNS 316**

This section pertains to criminal breach of trust.

#### **IPC Section 411/BNS 317**

This section deals with dishonestly receiving stolen property.

**IT Act Section 66** – Computer related offences

**IT Act Section 66** – This section addresses identity theft and unauthorized use of electronic signatures, passwords, or any other unique identification feature.

**IT Act Section 66D** – This section pertains to cheating by personation using computer resources.

Lost cell phone, it may affect your cells and hormone



## EXAM MALPRACTICE

Examination malpractice is defined as any deliberate act of wrongdoing, contrary to the rules of examinations designed to give a candidate an undue advantage. Also known as cheating, these days students resort to hi-tech examination malpractice (otherwise called e-cheating or digital cheating) in various levels of the educational system.

### IT Sections Applicable

**Information Technology Act, 2000 – Section 66:** This section deals with computer-related offenses, including unauthorized access to computer systems.

**Information Technology Act, 2000 – IPC Section 43:** This section covers penalties for unauthorized access, damages to computer systems, and data breaches.

**Indian Penal Code, 1860 – IT Act Section 420:** This section deals with cheating and dishonestly inducing delivery of property.

**Prevention of Unfair Means Act (PUMA):** While not a cyber law, this act is irrelevant as it addresses unfair practices during exams.

**UGC Regulations / University Rules:** Universities and educational institutions often have their own rules and regulations to prevent exam malpractice.

**Short cuts may cut short your career.**

## CONNECTED CAR

Connected cars are part of the 'internet of things', a phrase that refers to everyday items being connected to the internet with the intention of making life easier. The connected car is becoming software-defined, network-aware, and ultra-connected, transmitting data and "interacting" with the road and every other vehicle around it, increasing the chances of getting hacked!

### IT Sections Applicable

**IPC Section 354D/BNS 78** – This Section also covers online stalking that is to say monitoring her use of the internet, email or other forms of electronic communications & 66 R/W 43 (a), if he causes DOS then 43(f).

**Information Technology Act, 2000 :**

**IT Act Section 43** – Unauthorized access to computer systems and data.

**Section 66** – Computer-related offenses, including hacking and data theft.

**IT Act Section 66B** – Punishment for dishonestly receiving stolen computer resources or communication devices.

**Motor Vehicles Act, 1988 :**

Various sections related to road safety, licensing, registration, and liability in case of accidents involving connected vehicles.

**Privacy Laws :**

Personal Data Protection Bill (proposed) or any relevant amendments to existing laws. These laws would govern the collection, storage, processing, and sharing of personal data by connected vehicles.

**Consumer Protection Laws :**

Consumer Protection Act, 2019: Pertinent sections related to product liability and consumer rights in case of defects or malfunctions in connected car systems.

**While using IoT-Internet of Things also use your IoT-Intelligence of Thinking.**

## DRUG TRAFFICKING

The last decade has seen the emergence of new internet technologies that have acted as important facilitators of online drug markets. The internet now hosts a range of virtual marketplaces (both on the surface and deep web) for selling and buying illicit substances. Greater connectivity, global outreach and easily accessible forums are some of the reasons for their popularity.

### IT Sections Applicable

Sections of NDPS (sections would apply depending upon the quantity that she was in possession of at the time of the raid, it could be for personal consumption or commercial quantity, and sections would also apply as to whether she was also supplying or trading/dealing/facilitating of the banned substances)

#### **NDPS Act:**

- Section 8(c)** – Prohibition of Certain Operations
- Section 18** – Punishment for contravention in relation to manufactured drugs and preparations
- Section 21** – Punishment for contravention in relation to poppy straw
- Section 27A** – Punishment for financing illicit traffic and harbouring offenders

**Use of prohibited drugs when depressed, you may have your freedom to right to life and right to personal liberty get suppressed.**

## DOXING

To dox someone means to release their personal or private information that may prove harmful or embarrassing. This can happen in the real world, but the internet has made it easier both to find and release this information to a wide audience. Doxing may reveal someone's personal information like their home address or workplace, social security or phone number, private correspondence or pictures, criminal history, IP address, or other details.

### IT Sections Applicable

**IT Act Section 66C – Identity Theft (Information Technology Act, 2000):** This section deals with the punishment for identity theft.

**IT Act Section 66D – Cheating by Personation (Information Technology Act, 2000):** This section addresses the offense of cheating by personation using a computer resource

**IT Act Section 72 – Breach of Confidentiality and Privacy (Information Technology Act, 2000):** This section deals with the punishment for unauthorized access to computer material, including personal data, and the breach of confidentiality and privacy.

**IPC Section 354D/BNS 78 – Stalking (Indian Penal Code, 1860):** While not specific to cyber crime, this section criminalizes stalking

**IPC Section 509/BNS 79 – Word, Gesture or Act Intended to Insult the Modesty of a Woman (Indian Penal Code, 1860):** Again, not specific to cyber crime, this section could be relevant if the doxing includes the sharing of explicit or private material with the intent to insult or harm the victim.

**As in Boxing, in Doxing too an accused could launch a knockout punch causing irreparable injury to the victim.**

## CYBER GROOMING

Cyber grooming is the process of 'befriending' a young person online "to facilitate online sexual contact and/or a physical meeting with them with the goal of committing sexual abuse. Cyber grooming is when someone (often an adult) befriends a child online and builds an emotional connection with future intentions of sexual abuse, sexual exploitation or trafficking. The main goals of cyber grooming are: to gain trust from the child, to obtain intimate and personal data from the child (often sexual in nature—such as sexual conversations, pictures, or videos) in order to threaten and blackmail for further inappropriate material.

### IT Sections Applicable

**Sections of POCSO,**

**IPC Section 292/BNS 294**

**IT Act Section 66E – Violation of Privacy:** This section deals with capturing, transmitting, or publishing private images of a person without their consent, leading to the violation of their privacy

**IT Act Section 67B – Publishing or Transmitting Obscene Material:** This section addresses the publishing or transmitting of sexually explicit material, including messages, images, or videos, which can be used as tools for grooming activities.

**IT Act Section 67C – Preservation and Retention of Information by Intermediaries**

**IT Act Section 67A – Punishment for Publishing or Transmitting of Material Containing Sexually Explicit Act**

**IT Act Section 67 – Publishing or Transmitting of Material Containing sexually explicit act, etc. in electronic form**

**Browse the internet with utmost Morality (principles concerning the distinction between right and wrong or good and bad behaviour) else you are sure to be encountered with cyber crimes with Mathematical Certainty.**

## CRYPTO FRAUDS

Scammers are always looking for new ways to steal your money, and the massive growth of crypto currency in recent years has created plenty of opportunities for fraud. There are many types of crypto scams. Some of the most common include: Fake Websites, Pump and Dump Scams, Phishing Scams, Fake Apps, Fake celebrity endorsements, Giveaway scams, cloud mining scams and initial offering scams.

### IT Sections Applicable

**IT Act Section 43(a)** – This section deals with unauthorized access to computer systems and data breaches

**IT Act Section 66C** – This section pertains to identity theft and could be applied to cases where individuals' identities are stolen for fraudulent purposes related to crypto currencies.

**IT Act Section 66D** – This section addresses cheating by personation by using computer resources and communication devices.

**IPC Section 420/BNS 318** – Although not part of the IT Act, Section 420 of the IPC covers cheating and dishonestly inducing delivery of property.

**Check your Avenues (a strategy for making money, a financial approach or method) else there could be reduction in your Revenues.**

## CYBER SEX TRAFFICKING

Cyber sex trafficking, or online sexual exploitation, is a cyber crime and a form of modern slavery. Cyber sex trafficking is when a victim is forced into sexual exploitation using coercion, force, or fraud, and their abuse is streamed live on the internet via webcam, video, photography, or other digital media.

### IT Sections Applicable

**IPC Section 499/BNS 356, IPC Section 506/BNS 351, IPC Section 509/BNS 79, IPC Section 354A/BNS 75, IPC Section 370/BNS 143, 347 IPC Section 347/BNS 127, 357 IPC Section 357/BNS 135**

**IPC Section 370A** – Trafficking of persons for exploitation, which includes trafficking for sexual exploitation through electronic means. Disclosing sexually explicit or filthy content Section 292 of IPC.

Sections of Immoral Traffic (Prevention) Act 1956 also known as PITA (Prevention of Immoral Trafficking Act).

### **67 & 67A IT Act:**

**IT Act Section 67B** – Prohibition of publishing or transmitting sexually explicit material in electronic form, which includes content that promotes or facilitates cyber sex trafficking.

**While surfing the internet and making connections, be Mindful else it could take you from Sublime to Ridicule (from something that is very good or very serious to something very bad or silly).**

## CYBERWARFARE

Cyberwarfare is the use of cyber attacks against an enemy state, causing comparable harm to actual warfare and/or disrupting vital computer systems. Some intended outcomes could be espionage, sabotage, propaganda, manipulation or economic warfare.

### IT Sections Applicable

**IT Act Section 43** – Deals with unauthorized access to computer systems and data breaches.

**IT Act Section 66** – Addresses computer-related offenses, including hacking.

**IT Act Section 66F** – Focuses on cyber terrorism, which can be relevant to cyber warfare activities.

**IT Act Section 70 A** – This section was introduced through an amendment in 2008 to provide the government with powers to issue directions for ensuring the security of cyberspace. It empowers the government to take measures for identification, analysis, and prevention of cyber threats.

**IT Act Section 69** – This section grants the Indian government the power to intercept, monitor, and decrypt any information generated, transmitted, received, or stored in any computer resource if it is necessary for national security or for maintaining public order.

### **IPC Section 121/BNS 147. 66E, 66 R/W 43(a) (c) (e) (f)**

Sections of Unlawful Activities (Prevention) Act, 1967 (UAPA).

In Maharashtra- Sections of The Maharashtra Control of Organised Crime Act, 1999 (MCOCA).

Sections of Prevention of Terrorism Act, 2002.

**Right to Remedy shall be Rejected if for the offence of Hacking an accused gets Convicted.**



## HACKTIVISM

Derived from combining the words 'Hack' and 'Activism', hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes. The individual who performs an act of hacktivism is said to be a hacktivist. The hacktivist who does such acts, such as defacing an organization's website or leaking that organization's information, aims to send a message through their activities and gain visibility for a cause they are promoting.

### IT Sections Applicable

**Information Technology Act, 2000 – Section 43:** This section deals with unauthorized access to computer systems, data, or networks.

**Information Technology Act, 2000 – Section 66:** This section addresses computer-related offenses, including hacking and unauthorized access.

**Information Technology Act, 2000 – Section 66F:** This section specifically targets cyber terrorism and related activities.

**Information Technology Act, 2000 – Section 70:** This section empowers the government to secure cyberspace by issuing directions for the interception, monitoring, or decryption of any information through any computer resource.

**IPC Section 120A/BNS 61, IPC Section 121/BNS 147**

**IPC Section 122/BNS 149, IPC Section 153/BNS 192**

**IPC Section 153A/BNS 196, IPC Section 107/BNS 45**

**Think about you and do not allow someone else to think for you.**

## METaverse

The metaverse is a 3D version of the Internet and computing at large. The metaverse is "an integrated network of 3D virtual worlds." These worlds are accessed through a virtual reality headset – users navigate the metaverse using their eye movements, feedback controllers or voice commands. The headset immerses the user, stimulating what is known as presence, which is created by generating the physical sensation of actually being there.

### IT Sections Applicable

#### **IPC Section 354/BNS 74, IPC Section 506/BNS 351 sections of POCSO, section 67B IT Act**

Right to Privacy is now a Fundamental Right under Article 21 of the Constitution of India.

**Data Protection and Privacy Laws:** Laws regulating the collection, storage, processing, and sharing of personal data could apply to user interactions within the metaverse. In India, this might include compliance with the Personal Data Protection Bill, once enacted into law.

**Intellectual Property Laws:** Laws governing copyrights, trademarks, and patents could extend to creations within the metaverse, such as virtual goods, artwork, and designs.

**Online Conduct and Harassment Laws:** Just as in the real world, laws against harassment, hate speech, and cyber bullying could apply to interactions in the metaverse.

**Digital Transactions and Consumer Protection Laws:** If virtual goods and services are bought and sold within the metaverse, laws related to digital transactions and consumer rights might be relevant.

**Cyber security Laws :** Laws related to cyber security and hacking could apply to unauthorized access, data breaches, and other security incidents within the metaverse.

**Be well versed that Metaverse is not the real Universe.**

## SESSION HIJACKING ATTACK

In a session hijacking attack, cyber criminals gain unauthorized access to an active user session by exploiting vulnerabilities in web applications or networks. By taking control of the session, they can impersonate the user, access sensitive information, or conduct unauthorized actions, compromising the user's privacy and security.

### IT Sections Applicable

**IT Act Section 43** – This section deals with unauthorized access to computer systems, data theft, and other computer-related offenses.

**IT Act Section 66C** – This section specifically addresses identity theft. If a session hijacking attack is carried out with the intention of impersonating an individual or causing financial or reputational harm to them, this section could be invoked.

**IT Act Section 66D** – This section covers cheating by impersonation using a computer resource.

**IT Act Section 66E** – This section deals with violation of privacy.

**IT Act Section 72** – This section protects the confidentiality and privacy of information handled by service providers.

**Don't let cyber intruders hijack your online ride;  
secure your sessions and protect your stride.**

## PROMPT ENGINEERING

Prompt engineering refers to the manipulation of users through carefully crafted messages or prompts to deceive them into revealing sensitive information or performing unintended actions. This social engineering technique is commonly used in phishing attacks, where cyber criminals trick individuals into disclosing passwords, personal data, or financial details.

### IT Sections Applicable

- IT Act Section 43** – Unauthorized access to computer systems.
- IT Act Section 66** – Computer-related offenses, including hacking.
- IT Act Section 67** – Punishment for publishing or transmitting obscene material in electronic form.
- IT Act Section 69** – Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
- IT Act Section 72** – Breach of confidentiality and privacy.
- IT Act Section 79** – Intermediaries not to be liable in certain cases.
- IT Act Section 84A** – Modes or methods for encryption. The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.
- IT Act Section 85** – Offenses by companies.

**Stay cautious and alert, so prompt engineering won't make you divert.**

## FILELESS ATTACKS

This attack evades traditional antivirus and detection systems by executing malicious code directly in computer memory, without leaving traces on the file system. These stealthy attacks exploit vulnerabilities in software, making them harder to detect and providing cyber criminals with remote access to systems for data theft, surveillance, or launching further attacks.

### IT Sections Applicable

**IT Act Section 43 (Unauthorized Access)** – This section deals with unauthorized access to computer systems, data, or networks.

**IT Act Section 43A (Compensation for Data Breach)** – This section deals with the compensation for improper disclosure of personal information.

**IT Act Section 66 (Computer-Related Offenses)** – This section covers various computer-related offenses, including hacking.

**IT Act Section 66B (Punishment for Receiving Stolen Computer Resources or Communication Devices)** – If fileless attacks involve receiving stolen computer resources or communication devices, this section might be invoked.

**IT Act Section 66C (Identity Theft)** – If a fileless attack leads to identity theft, this section might apply.

**IT Act Section 66E (Violation of Privacy)** – In cases where privacy is violated through fileless attacks, this section might be invoked.

**IT Act Section 66F (Cyber Terrorism)** – If the fileless attack is carried out with the intent of causing terror or destabilizing critical infrastructure, this section could apply.

**Silent and sneaky, fileless foes;  
fortify your defenses and block their throes.**

## DELIVERY SCAM

A delivery scam involves cyber criminals sending fake notifications or tracking information to deceive recipients into believing they have a package or delivery pending. The scam aims to trick victims into revealing personal information, clicking on malicious links, or paying fake shipping fees, leading to financial loss or data compromise.

### IT Sections Applicable

- IT Act Section 43** – Penalty for unauthorized access, damage to computer systems, etc.
- IT Act Section 66** – Computer-related offenses, including cheating by personation using a computer resource.
- IPC Section 419/BNS 319** – Punishment for cheating by personation.
- IPC Section 420/BNS 318** – Cheating and dishonestly inducing delivery of property.

**Don't fall for the scammer's snare;  
verify before you click 'Accept' or 'Share'.**

## VIRTUAL KIDNAPPING

This is a psychological extortion scheme where perpetrators manipulate victims into believing a loved one has been kidnapped, demanding ransom to ensure their release. Though no actual abduction occurs, the emotional distress and fear generated can lead victims to comply with the demands.

### IT Sections Applicable

#### **Information Technology Act, 2000**

**IT Act Section 66C** – This section deals with identity theft, which could be relevant if someone's identity is misused in a virtual kidnapping scenario.

**IT Act Section 66D** – This section covers cheating by impersonation using a computer resource, which could apply if the perpetrator impersonates the victim.

#### **Indian Penal Code (IPC)**

##### **IPC Section 503/BNS 351**

This section deals with criminal intimidation, which could be relevant if threats are made in a virtual kidnapping scenario.

##### **IPC Section 506/BNS 351**

This section deals with criminal intimidation by threat of injury to a person's reputation, etc.

**Guard your virtual realm with might;  
virtual kidnappers shall lose the fight.**

## FORMJACKING

It is an attack that involves injecting malicious code into e-commerce websites' payment forms. The code steals payment card details or personal information entered by customers during online transactions, allowing cyber criminals to engage in payment fraud or identity theft.

### IT Sections Applicable

#### **Information Technology Act, 2000:**

- IT Act Section 43** – This section deals with unauthorized access to computer systems and data breaches.
- IT Act Section 43A** – This section deals with the compensation for failure to protect sensitive personal data.
- IT Act Section 66** – This section deals with computer-related offenses, including hacking.
- IT Act Section 66C** – This section deals with identity theft.

#### **Indian Penal Code, 1860:**

- IPC Section 420/BNS 318** – This section deals with cheating and dishonestly inducing delivery of property.
- IPC Section 463/BNS 336** – This section deals with forgery.
- IPC Section 464/BNS 335** – This section deals with making a false document.

**Protect your forms with utmost care;  
formjackers won't find their share.**



## CYBERSQUATTING

It refers to the practice of registering domain names similar to established brands or trademarks with the intent to profit from the brand's reputation or sell the domain back to the rightful owner at an inflated price. This can lead to brand dilution, reputation damage, and confusion among consumers.

### IT Sections Applicable

- IT Act Section 2(1)(r)** – Defines "domain name," which is crucial in understanding the context of cybersquatting.
- IT Act Section 43** – This section deals with penalties and compensation for damage to computer systems
- IT Act Section 66–D** – This section covers the offense of cheating by impersonation using a computer resource
- IT Act Section 66–A** – Although this section was struck down by the Supreme Court of India in 2015 for being unconstitutional,
- IT Act Section 79** – While not directly focused on cybersquatting, this section deals with intermediary liability.
- IT Act Section 81** – This section ensures that the provisions of the IT Act have an overriding effect, not withstanding anything inconsistent in any other law for the time being in force.

**Stake your claim in the digital space;  
cybersquatters will find no place.**

## DNS HIJACKING

This attack involves altering the Domain Name System (DNS) settings of a computer or network, redirecting legitimate traffic to malicious websites. By intercepting and manipulating DNS queries, attackers can lead users to phishing pages, distribute malware, or engage in other malicious activities.

### IT Sections Applicable

- IT Act Section 43** – This section deals with unauthorized access to computer systems and data.
- IT Act Section 66** – This section deals with computer-related offenses like hacking, which could cover unauthorized access, interference, or damage to computer systems.
- IT Act Section 66C**– This section deals with identity theft. If someone uses another person's identity to commit an offense related to DNS hijacking, this section could be invoked.
- IT Act Section 66D** – This section covers cheating by personation using computer resources.
- IT Act Section 66E**– This section deals with violation of privacy.
- IT Act Section 72** – This section protects the privacy and confidentiality of information stored in a computer resource.

**Don't let your online path divert; secure your DNS, stay alert.**

## SMS BOMBING

It is a form of harassment where attackers overwhelm a victim's mobile device with a large number of unwanted text messages, disrupting normal communication and potentially causing psychological distress. This attack aims to disrupt the victim's peace of mind or sabotage their ability to use their phone.

### IT Sections Applicable

**IT Act Section 66C – Identity theft :** This section deals with punishment for identity theft, which includes dishonestly using another person's electronic signature, password, or any other unique identification feature.

**IT Act Section 66D – Cheating by personation using computer resource :**

This section addresses the act of cheating by personation using a computer resource, and it prescribes penalties for such actions.

**IT Act Section 43 – Penalty and compensation for damage to computer, computer system, etc. :** This section deals with penalties for unauthorized access to computer systems, data breaches, and causing damage to computer resources.

**IT Act Section 66 – Computer-related offenses :** This section covers various offenses related to computer systems, including hacking, unauthorized access, and introduction of viruses.

**Bombarded by texts, it's no fun;  
safeguard your phone, block the SMS gun.**

## INSIDER THREATS

Refers to security risks posed by individuals with legitimate access to an organization's systems, networks, or sensitive information. These threats may arise from employees, contractors, or business partners who intentionally or unintentionally misuse their privileges to steal data, commit fraud, or compromise the organization's security.

### IT Sections Applicable

<b>IT Act Section 43A</b>	- Compensation for Data Breach
<b>IT Act Section 66C</b>	- Identity Theft
<b>IT Act Section 66D</b>	- Cheating by Personation by using Computer Resource
<b>IT Act Section 72</b>	- Breach of Confidentiality and Privacy
<b>IT Act Section 72A</b>	- Punishment for Disclosure of Information in Breach of Law
<b>IPC Section 408/BNS 316</b>	- Criminal Breach of Trust by Clerk or Servant

**Be cautious of those who reside within;  
trust but verify, and potential harm will thin.**

## FAKE INFLUENCER SCAM

A fake social media influencer lures followers with giveaways and luxury brand deals. Victims pay registration fees but never receive prizes. The influencer vanishes after collecting money.

### IT Sections Applicable

#### **IT Act, 2000:**

**Section 66D** - Cheating by personation using a computer resource

**Section 79** - Liability of intermediaries for hosting fraudulent content

#### **IPC / BNS:**

**Section 419 / BNS 319(2)** - Punishment for cheating by personation

**Section 420 / BNS 318(4)** - Cheating and dishonestly inducing delivery of property

**Section 468/ BNS 336(3)** - Forgery for purpose of cheating

#### **Consumer Protection Act, 2019:**

**Section 2(47)** - Misleading advertisements

**Section 21** - Penalties for false endorsements

**Following fake fame can lead to real fraud!**

## DIGITAL ARREST

A scammer posing as a police officer threatens victims with fake criminal charges. They demand immediate payment to "settle" the case. Victims panic and transfer money, only to realize there's no such legal provision.

### IT Sections Applicable

#### **IT Act, 2000 :**

**Section 66C** - Identity theft

**Section 66D** - Impersonation using a computer resource

#### **IPC / BNS:**

**Section 170 / BNS 204** - Personating a public servant

**Section 171 / BNS 205** - Wearing garb or carrying a token used by a public servant

**Section 383/ BNS 308** - Extortion

#### **Indian Evidence Act, 1872:**

**Section 65B** - Admissibility of electronic records as evidence in fraud cases

#### **BSA, 2023:**

**Section 63** - Admissibility of electronic records as evidence in fraud cases

**If WhatsApp says you're under arrest,  
reply with a lawyer emoji and block!**

## JUMPED DEPOSIT

A scammer claims to have sent extra money to a seller and fakes a bank notification. The seller, believing the transaction is real, refunds the excess amount. Later, they discover no deposit was made.

### IT Sections Applicable

**IT Act, 2000 :**

**Section 66D** – Cheating by personation using a computer resource

**Section 43** – Unauthorized access and fraud

**IPC / BNS:**

**Section 406 / BNS 316(2)** – Criminal breach of trust

**Section 417/ BNS 318/(2)** – Cheating

**Section 420/ BNS 318(4)** – Cheating and dishonestly inducing delivery of property

**Consumer Protection Act, 2019:**

**Section 74** – Unfair trade practices

If it's too jumpy to track,  
it's too risky to pay!

## CALL MERGE SCAM

A fraudster calls a victim, pretending to be from the bank. They ask the victim to merge another call, where an accomplice requests an OTP. The scammer secretly listens, steals the OTP, and empties the victim's account.

### IT Sections Applicable

#### **IT Act, 2000:**

- Section 66C** – Identity theft
- Section 66D** – Cheating by personation

#### **IPC / BNS:**

- Section 420 / BNS 318(4)** – Cheating
- Section 468 / BNS 336(3)** – Forgery for purpose of cheating
- Section 511/ BNS 62** – Attempt to commit offenses punishable with life imprisonment

#### **Telegraph Act, 1885:**

- Section 25** – Unauthorized interception of messages

**Three's not company  
when the third one's a fraudster!**



## MALVERTISING

Clicking on an online ad for discounts or free products can install malware. The malicious ad redirects users to fake sites that steal login details. Victims lose money or have their data compromised.

### IT Sections Applicable

#### **IT Act, 2000:**

- Section 43** – Unauthorized access and damage to computer systems
- Section 66** – Hacking and fraudulent use of computer resources
- Section 69A** – Blocking of harmful content

#### **IPC / BNS:**

- Section 425/ BNS 324** – Mischief
- Section 426/ BNS 324(2)** – Punishment for mischief

#### **Consumer Protection Act, 2019:**

- Section 89** – Deceptive online advertising penalties

**Those flashy ads could flash your data too!**

## WATERING HOLE ATTACK ■

Hackers infect a trusted website frequently visited by a specific group. When users access the site, their devices get compromised. Cyber criminals steal credentials or install spyware without the victim's knowledge. ■

### IT Sections Applicable

#### **IT Act, 2000:**

- Section 43** – Unauthorized access
- Section 66** – Hacking with intent to cause harm
- Section 72** – Breach of confidentiality and privacy

#### **IPC / BNS:**

- Section 426 / BNS 324(2)** – Mischief
- Section 471 / BNS 340(2)** – Using forged document as genuine
- Section 120B / BNS 61(2)** – Criminal conspiracy

**Even safe-looking sites might be  
poison puddles – tread carefully**

## LLM JAILBREAK

A user manipulates an AI chatbot to bypass safety rules. The AI shares restricted information like hacking techniques. Authorities track misuse, and the user unknowingly becomes part of a cyber crime investigation.

### IT Sections Applicable

#### **IT Act, 2000:**

- Section 66** – Hacking and system manipulation
- Section 67B** – Publishing harmful content
- Section 69** – Government access and control over AI misuse

#### **IPC / BNS :**

- Section 505 / BNS 353** – Statements conducing to public mischief
- Section 120B / BNS 61(2)** – Criminal conspiracy

#### **Copyright Act, 1957:**

- Section 51** – Infringement of copyright through AI-generated content

**Don't teach the bot to be bad**  
**- it might graduate with honors in hacking!**

## FAKE NEWS

A communal rumor about a violent incident spreads rapidly online. People react emotionally and forward false information. Chaos ensues before authorities confirm the news was fake.

### IT Sections Applicable

#### **IT Act, 2000:**

**Section 69A** – Blocking of information in public interest

**Section 66F** – Cyber terrorism if fake news incites violence

#### **IPC / BNS:**

**Section 153A / BNS 196** – Promoting enmity between groups

**Section 505 / BNS 353** – Statements conducing to public mischief

**Section 124A** – Sedition, if applicable (This section is deleted in BNS 2023)

#### **Press Council Act, 1978:**

**Section 14** – Powers of the Press Council to address fake news

**Not every forwarded message is the gospel**  
– sometimes it's gossip!

## FAKE PRODUCTIVITY APPS

An app claiming to improve focus or time management secretly collects user data. Once installed, it asks for excessive permissions and starts spying on calls and messages. Victims lose privacy and sensitive information.

### IT Sections Applicable

#### **IT Act, 2000:**

- Section 43** – Unauthorized data collection and misuse
- Section 66** – Computer-related offenses
- Section 72** – Breach of privacy

#### **IPC / BNS:**

- Section 420 / BNS 318(4)** – Cheating
- Section 468 / BNS 336(3)** – Forgery for fraud
- Section 120B / BNS 61(2)** – Criminal conspiracy

#### **Consumer Protection Act, 2019:**

- Section 10** – Product liability for defective digital services

**If the app promises too much,  
it's probably taking more than your time!**

## STEGANOGRAPHY

A seemingly harmless image file hides malicious code. When downloaded or opened, malware gets installed on the device. Cyber criminals use this technique to spread spyware and steal information.

### IT Sections Applicable

#### **IT Act, 2000:**

- Section 66F** – Cyberterrorism if used for extremist purposes
- Section 69** – Government's power to decrypt and monitor
- Section 72** – Breach of confidentiality and privacy

#### **IPC / BNS:**

- Section 201 / BNS 238** – Causing disappearance of evidence
- Section 120B / BNS 61(2)** – Criminal conspiracy
- Section 124A** – Sedition, if applicable (This section is deleted in BNS 2023)

#### **Official Secrets Act, 1923:**

- Section 3** – Espionage using steganography

**If a file looks innocent but acts guilty,  
it's steganography in disguise!**