

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:

- | | |
|---------------------------|-----------------------------|
| IT Act Section 43 | – Unauthorized Access |
| IT Act Section 66 | – Computer related offences |
| IT Act Section 66C | – Identity Theft |
| IT Act Section 66D | – Cheating by Personation |
| IT Act Section 66E | – 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.