

# Are Doctors Easy Targets for Cyber Frauds?

Sadananda B Naik<sup>1</sup>, Sangram Biradar<sup>2</sup>

## ABSTRACT

Doctors seem to be a soft target for the scamsters for cyber frauds. We are otherwise known for our intelligence and shrewdness, fall prey to these cyber criminals with ease. This is a short write-up on this very problem.

**Keywords:** Cyber frauds, Digital arrest, Doctors.

*Bengal Physician Journal* (2025): 10.5005/jp-journals-10070-8081

Doctors who are otherwise very intelligent tribe with above average IQ, find themselves wanting, when it comes to responding to legal notices or notifications, be it by post or by mail from the law enforcing authorities or statutory bodies. Doctors who fight tooth and nail when it comes to academics to justify their views or oppose others, the ones who do not take anything lying in medical science without robust evidence and literature support, but simply panic when it comes to responding to legal notices. Doctors on seeing a legal notice addressed to them, go into a state of utter shock and fear. They simply panic and fail to apply any common sense in dealing with them. They believe the contents of legal documents as real without any minimal effort to confirm the authenticity of such mails or messages. They do not even care to share the contents of the message or mail with their beloved family members or close friends. This weakness seems to be the main reason for the doctors to fall prey to cyber frauds. By the time the doctors let their friends and relatives know about the goof-up, it would be too late for any remedial measures. Thousands of doctors trying to enter their personal data and other professional details to register themselves using a fake NMC registration link is the latest example for such knee-jerk response without verifying its authenticity.<sup>1</sup> In this article, we have tried to address a more serious issue of cybercrimes and frauds where hundreds of doctors are targeted on a regular basis, so that doctors are aware of the digital scam scenario, modus operandi, and available legal remedies if they fall victim.

## MODUS OPERANDI

- The doctor receives a call from fraudsters, who would pose as Central Bureau of Investigation (CBI) officials, and informs the doctor that a new bank account had been opened in his name by one xxxx and the account was used for various criminal activities, including bank fraud and money laundering. After that they would ask for the doctor's "Aadhaar" details and enquire about the amount of money in the bank account. They would then threaten the doctor that action would be taken against him unless he transfers a sum of money to them and compel the doctor to transfer money to him in installments to several different bank accounts belonging to the fraudsters, only to realize the fraud later and he then files a police complaint.<sup>2</sup>
- Anonymous caller identifying himself as an employee of a xxx bank where the doctor is holding his savings account and dupes him to divulge his personal details like PAN, AADHAR, etc. The doctor would get a text message that his bank account will

<sup>1</sup>Department of Internal Medicine, Alvas Health Centre, Moodabidri, Karnataka, India

<sup>2</sup>Department General Medicine, M.R. Medical College, Gulbarga, Karnataka, India

**Corresponding Author:** Sadananda B Naik, Department of Internal Medicine, Alvas Health Centre, Moodabidri, Karnataka, India, Phone: +91 9845051005, e-mail: sadanandanaik2@gmail.com

**How to cite this article:** Naik SB, Biradar S. Are Doctors Easy Targets for Cyber Frauds? *Bengal Physician Journal* 2025;12(1):34–37.

**Source of support:** Nil

**Conflict of interest:** None

be suspended soon unless he updates his KYC using the link messaged or mailed. Now the doctor believes the message and clicks the link to update PAN details and soon disastrous consequences occur ending in a huge sum of money getting debited from the bank account.<sup>3</sup>

- The doctor receives a call from an unknown number and the caller introduces himself as xxxxx, an inspector from Crime Branch, Mumbai, and he then informs that his bank account has been used for illegal transactions involving huge amounts. He would console him as "Though you have not committed any crime, you must cooperate with the investigation" And then the imposter asks the doctor to furnish details of fixed deposits made in various banks, and the doctor provides him the information on all the fixed deposits in the banks and transfers the money to a bank account number provided. The doctor realizes very late that he has been duped and then approaches the cyber economic and narcotics crime (CEN) Police Station.<sup>4</sup>
- The doctor gets an unknown call, where the caller identifies himself as an officer from the telecom department and informs him that an FIR has been booked against him for viewing and forwarding porn videos. The scamster then connects the doctor to a police officer from Mumbai's xxx Police Station and a police officer in uniform informs the doctor that an arrest warrant has been issued for sharing porn videos against him. The officer also informs the doctor that he has been charged in a money laundering case connected to Jet Airways founder Naresh Goyal and the National Security Act had been invoked on her/him, and if he/she transfers all her funds to their bank account, there can be some hope of getting out of this serious crime.

The panic-stricken doctor transfers a huge sum of money to the bank account shared by the police. Throughout the process, the doctor would be instructed to remain on WhatsApp video call, which the fraudsters describe as “Digital Arrest” and the hapless doctor obliges. The doctor files a complaint with the police later.<sup>5</sup>

- The doctor receives a call from an unknown person and the caller claims to be an officer from Customs and tells the doctor that the latter’s Aadhaar card had been used to book a courier in which five passports, five ATM cards, 200 grams of synthetic narcotic drug methylenedioxymethamphetamine (MDMA), and \$5,000 were found. When the doctor denies booking any article, the call would be then forwarded to another person who claimed to be a senior Customs officer and tells the Dr. that he received a complaint about the misuse of the doctor’s Aadhaar card. The doctor believes the fraudsters in this regard, and the fraudsters make the doctor confine himself to a room in his house for several days [in the name of “digital arrest.” In the meantime, the scamsters force him to transfer funds to different bank accounts and then disappear.<sup>6</sup>
- In few other cases, the scamsters threaten the doctors by posing as employees of a courier company [FedEx, India Post, etc.] with the alleged seizure of a parcel booked in his/her name. They would then subject the doctor to digital arrest for several days and flees him large sums of money. Similarly, there are several other modus of operandi like sending legal notice by email for offenses under prevention of money laundering act (PMLA), protection of children from sexual offence (POSCO), income tax (IT) ACT, etc. and many others could receive a video with a nude lady and get a phone call blackmailing the doctor with AI-generated photos, etc.

### Digital Arrest

This is the latest method in which the scamsters threaten and rob money. The victim is forced to stay on video calls for hours and days until a huge sum of money is transferred to the fraudulently. In reality, there is not anything called “digital arrest” in law. The cybercriminals use AI-generated voice or video to convince the victims that a serious offense has been committed. The scamsters then make the victim buy a new phone to stay connected with them through WhatsApp or Skype. A court trial would be done and would last for a few days through these video calls. The victim is made to believe that the entire proceedings are real with judges, police, and CBI officials in the background of a courtroom. They would force the victim to transfer all his money to the so-called “government accounts”.<sup>7</sup>

As seen here, there are multiple signatories with several departmental stamps to convince the doctor about its authenticity (Fig. 1). In this instance, the good sense of the doctor prevailed and he did not respond to it and hence escaped scamming.

### The Common Laws Quoted by the Scamsters to Scare Doctors

- Prevention of Money Laundering Act, 2002 PMLA.
- Protection of Children from Sexual Offences (POCSO) Act, 2012.
- Child Sexual Abuse Material (CSAM), Juvenile Justice (Care and Protection of Children) Amendment Act, 2021.
- Income-tax act, 1961.
- Cyber Offences and Penalties under the IT Act, 2000 amended in 2008.
- Indian Penal Code (IPC)/Bharatiya Nyaya Sanhita (BNS).

### LEGAL AUTHORITIES TO INVESTIGATE OFFENSES UNDER THESE LAWS

- The Enforcement Directorate: The Enforcement Directorate in the Department of Revenue, Ministry of Finance, and the Government of India is responsible for investigating the offenses of money laundering under the PMLA.
- The National Commission for Protection of Child Rights (NCPCR), CBI, and Cyber Crime Cells are entrusted with investigating and combating child pornography.
- Section 78 in the Information Technology Act, 2000.

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Inspector shall investigate any offense under this Act.

### Remedies Available for Cyber Fraud Victims

*One can Report a Cyber Crime by:*

- Filing a written complaint in the nearest, Cyber Cell.
- Lodging an First Information Report (F.I.R).
- Filing a complaint at <https://www.cybercrime.gov.in/Accept.aspx>.

### Prevention of Cyber Frauds

Prevention is always better than cure, be it an illness or cyber fraud.

### Few Tips to Tackle Fraudulent Cyber Notices or Calls

- When a threat or notice is received either by phone or email, the first response is not to panic and act hastily.
- Identify the telltale signs of fraudulent notice namely multiple department seals/stamps, and multiple statutory laws quoted to implicate you.
- Do not oblige to transfer money at any cost.
- In case they threaten you not to divulge this to anyone, just ignore them and approach the cybercrime police @1930 without any delay.
- Then try to identify the caller using caller ID software.
- Ignore all the email notices irrespective of the office which is sending it.
- Report to cyber cells or the nearest police stations.
- Cybercriminals can pose like officials of any department like police, CBI, ED, IT officials, or officials of any other government agencies. They are always equipped with fake ID cards and fake office settings [in case of video calls].
- Guilty mind is more amenable to manipulation and panic, hence, even if you think that you have committed any of the alleged offenses, there are enough legal remedies available to defend you.
- If anyone asks to confirm your address or conducting a survey by opting to press 1 or 2, avoid obliging them, it is going to be a scam.
- If anyone demands to find the OTP that was sent to you, simply refuse to oblige avoid answering unknown video calls.

### Government Initiatives

- The Government of India has taken the issue very seriously and the Ministry of Home Affairs has tied up IITs, IIITs, and other top institutes to train the first batch of cyber commandos, as the special wing. The Government of India has drawn an initiative to formulate a core group of well-trained police officers, cyber commandos who will oversee the infrastructure on cyber securities.<sup>8</sup>



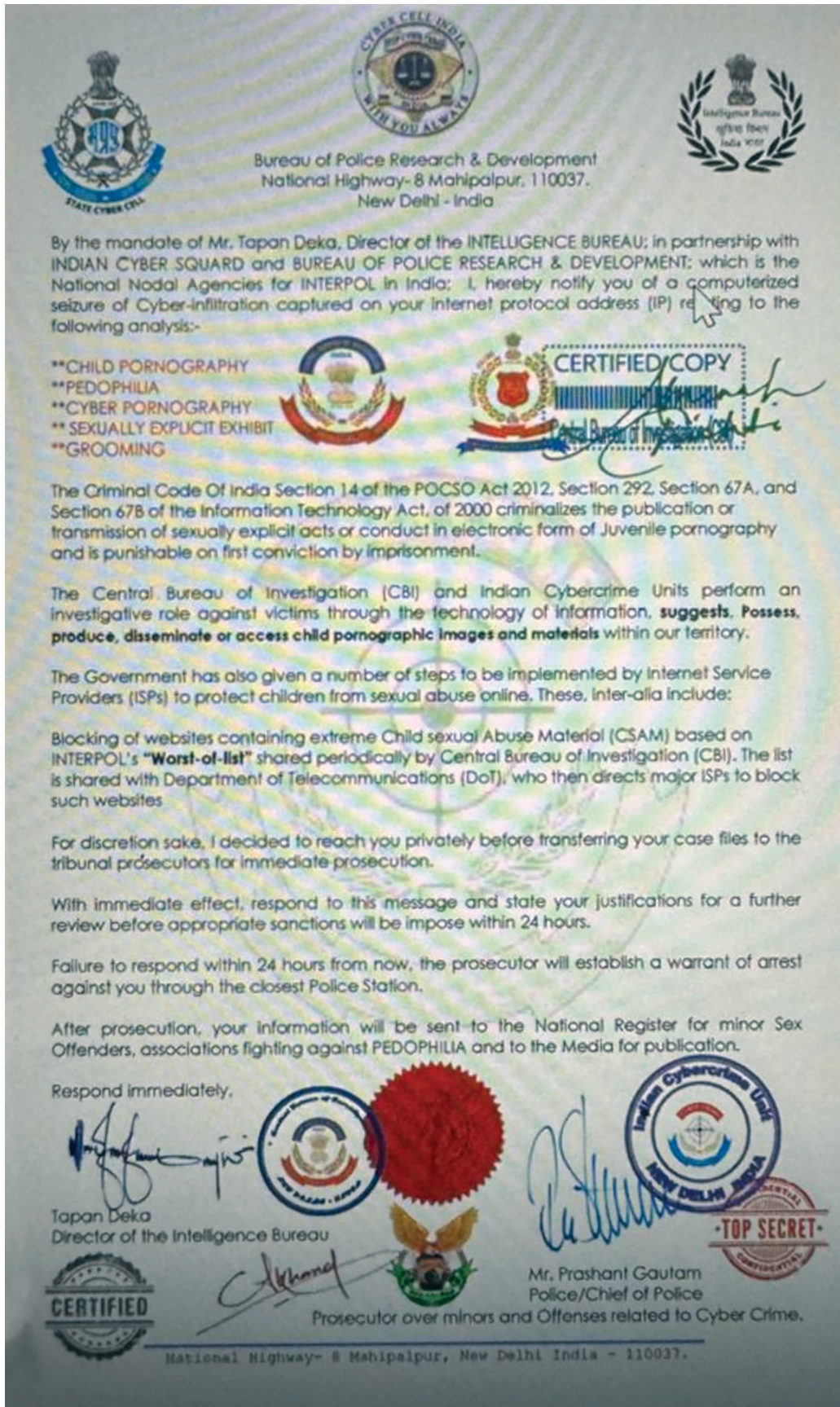


Fig. 1: Sample mail/letter

- The Karnataka State has strengthened the fight against digital fraud by creating a position for a dedicated Director General of Police (DGP), the first of its kind in the country, focused solely on cyber security. This move would help enhance the efficiency of the police department, especially in the field of investigation of cyber, economic, and narcotics crimes.<sup>9</sup>

## CONCLUSION

Unwarranted fear toward the investigation by the law-enforcing authorities like police, CBI, IT, CUSTOMS, ED, etc. seems to be the crux of the problem ailing the medical professionals who fall prey to cyber frauds. A sound knowledge and awareness of the legal remedies available and procedures to respond to notices from law enforcement authorities whether fraud or real is the need of the hour.

## ACKNOWLEDGMENTS

The authors are indebted to several blogs and social media posts which have inspired them while preparing the article.

## ORCID

Sadananda B Naik  <https://orcid.org/0000-0003-1960-7753>  
Sangram Biradar  <https://orcid.org/0000-0003-3840-1507>

## REFERENCES

1. Barsha Misra. Fact check: Beware of fake NMC link on social media asking doctors to register says State Medical Council. [Internet]. Mumbai: Medical Dialogues; 2023 [cited 2023 May 27]. Available from: <https://medicaldialogues.in/news/health/doctors/fact-check-beware-of-fake-nmc-link-on-social-media-asking-doctors-to-register-says-state-medical-council-112093>. [Last accessed on 27-2-2025].
2. Anagha. Elderly doctor in Karnataka duped of Rs 3.7 crore by 'fake' CBI officers. [Internet]. Haveri: India Today; 2024 [Cited 2024 May 22]. Available from: <https://www.indiatoday.in/india/karnataka/story/karnataka-haveri-doctor-duped-fake-cbi-officers-police-2542525-2024-05-22>. [Last accessed on 27-2-2025].
3. Subhendu Maiti. Cyber thugs cheat city doctor of Rs 4.5 lakh. [Internet]. Kolkata: The Statesman; 2024 [Cited 2024 April 10]. Available from: <https://www.thestatesman.com/bengal/cyber-thugs-cheat-city-doctor-of-rs-4-5-lakh-1503288833.html>. [Last accessed on 27-2-2025].
4. The Hindu Bureau. Fraudster impersonates police officer to dupe Dr. of ₹76.65 lakh. [Internet]. Kalaburagi: The Hindu; 2024 [Cited 2024 May 28]. Available from: <https://www.thehindu.com/news/national/karnataka/fraudster-impersonates-police-officer-to-dupe-dr-xxx-of-7665-lakh/article68225633.ece>. [Last accessed on 28-2-2025].
5. Abhishek De. Noida doctor duped of Rs 59 lakh after being put under 2-day 'digital arrest' [Internet]. New Delhi: India Today News Desk; 2024 [Cited 2024 Jul 25]. Available from: <https://www.indiatoday.in/india/story/noida-doctor-duped-digital-arrest-scam-cyber-crime-telecom-officials-2571781-2024-07-25>. [Last accessed on 28-2-2025].
6. The Hindu Bureau. Fraudsters virtually 'arrest' Udupi doctor, make away with ₹1.33 crore [Internet]. Mangaluru: The Hindu; 2024 [Cited 2024 August 14]. Available from: <https://www.thehindu.com/news/cities/Mangalore/fraudsters-virtually-arrest-udupi-doctor-make-away-with-133-crore/article68526041.ece>. [Last accessed on 28-2-2025].
7. Manish Dixit. Why Indians are falling easy prey to 'digital arrest' [Internet]. Lucknow: India Today; 2024 [Cited 2024 Sep 17]. Available from: <https://www.indiatoday.in/amp/india-today-insight/story/why-indians-are-falling-easy-prey-to-digital-arrest-2601475-2024-09-1>. [Last accessed on 28-2-2025].
8. Mukesh Ranjan. MHA ropes in IITs, IIITs, other top institutes to train first batch of cyber commandos [Internet]. New Delhi: THE NEW INDIAN EXPRESS; 2024 [Cited 2024 Aug 29]. Available from: <https://www.newindianexpress.com/amp/story/nation/2024/Aug/29/mha-ropes-in-iits-iiits-other-top-institutes-to-train-first-batch-of-cyber-commandos>. [Last accessed on 28-2-2025].
9. Nagarjun Dwarakanath. Karnataka becomes first state to create DGP role dedicated to cybersecurity [Internet]. Bengaluru: India Today; 2024 [Cited 2024 Nov 14] Available from: <https://www.indiatoday.in/india/karnataka/story/karnataka-becomes-first-state-in-india-to-create-dgp-role-cybersecurity-combat-rising-digital-crime-2633231-2024-11-14>. [Last accessed on 28-2-25].