COMMON CYBER THREATS

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

Here are some common forms of cyber threats to protect against.

RANSOMWARE

Malevolent software which locks user access by encrypting data using cryptovirology while extorting the payment from the victim in order to dencrypt and restore the files.

MALWARE

Malicious software installed on a machine unknowingly and performs criminal actions for a third party.

BOTNETS

A "secret key" that provides entry to devices and connections to be controlled by an attacker for criminal purpose.

SPOOFING

Email messages sent from a fraudulent account masquerading as a legitimate and trusted source as an attempt to gain access to a user's system or confidential information.

WORM

Stand alone software which does not require a host program in order to propagate and replicate itself onto other networks and drives damaging data and software as it spreads.

TROJANS

Computer program that contains destructive code disguised as the harmless programming.

DENIAL OF SERVICE {DDOS}

Floods bandwidth which makes online systems unavailable.

VIRUS

A type of malware that when executed spreads from computer by replicating its programming and infecting user programs and files to change the way they operate or to stop working altogether.

PHISHING

A DNS server software vulnerability is exposed or a host file is swapped and a legitimate website is maliciously redirected to a scan site where unknowing visitors enter their confidential information.

SPYWARE

Criminal malware on the hard drive used to covertly monitor user activities.

PHARMING

A DNS server software vulnerability is exposed or a host file is swapped and a legitimate website maliciously redirects to a scam site where unknowing visitors can enter into their own confidential information.

ADWARE

Can redirect the search requests or automatically render some of advertisements producing the revenue for its creator.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

PHISHING ATTACK ALERT

Gear up to protect yourself from cyber criminals.

TOP 5 RED FLAGS

- Web links can lead to unfamiliar sites (hover over them to check).
- There is an attachment you weren't expecting.
- You notice poor spelling & grammar throughout.
- It asks for personal info (passwords, all of bank information, etc.)
- The sender doesn't address you by name.

HOW TO STAY PROTECTED

1. Do not click on any links or attachments you can't verify
2. Call to verify requests for info (even if it seems to come from someone you know!)
3. Whenever in doubt, always contact optimal for help!

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

10 SECURITY TIPS FOR WORK FROM HOME

Use your workplace device having all of the security precautions in place.

Always use the two - factor - authentication and complex passwords for all accounts and devices.

Use VPN to access the data through secure connection.

Always enable the Data Loss Prevention (DLP) tools to ensure sensitive data is not lost.

Regularly update OS and Antivirus to protect against malware attacks.

Be aware of the COVID-19 scams, phishing, e-mails, malicious domains and fake apps.

Avoid using the unsecured, free, public wi-fi hotspot or network.

Ensure that only authentic verified URLs are accessed.

Regular backup of data in your system and cloud (One Drive, G-Drive, etc.).

Disable USB ports & System Bluetooth connectivity.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

THOUSANDS ARE FALLING PREY TO ONLINE JOB SCAMS EACH DAY. DON'T BE ONE OF THEM !

Here's how you can spot an internet job scam

- You are immediately selected for the Job.
- The interview is scheduled on the instant messaging platforms.
- Vague job requirement and job description.
- Search results about the Company or the job doesn't show up.
- Unprofessionally written e-mails.
- You are asked to provide Confidential Information.
- E-mails with no contact information or Company Signature.
- You're asked to Pay.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION

ADVOCACY ON DIGITAL SAFETY

STAY SECURE FROM IDENTITY FRAUD

How to safeguard yourself being an identity victim :

- Do not open short links that have been sent via e-mail or SMS.
- Update Antivirus software both on PC and Mobile phone.
- Don't communicate about financial / password information on e-mail or SMS.
- Do not post D.O.B, Birthplace or Mailing Address on Social Media Platforms.
- Change Passwords periodically.
- Don't have same format of passwords for all applications.
- Periodically check the Bank Statements and Credit Card Statements.
- Mention the purpose when you give Xerox copy of the PAN Card/Aadhar Card.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION

ADVOCACY ON DIGITAL SAFETY

CYBER SAFETY

How to stay safe online

Alawy keep your information & the passwords private

Be careful of what you are posting online

Always check your privacy settings

Shop safely on the trusted websites

Choose the strong passwords

Protect all of your devices with an antivirus

Remember to log off

Check the website url

Always check the e-mails before you open them

Avoid phishing & other scams

Always keep your children safe online

Respect yourself & others online

https://linktr.ee/endnowfoundation

END NOW FOUNDATION

ADVOCACY ON DIGITAL SAFETY

KEEPING YOUR SMARTPHONES & TABLETS SAFE !

Smartphones and Tablets need even more Protection than your 'Desktop' equipment.

Use 'Automatically Update' and keep your devices (and all installed apps) up to date.

Switch on the PIN / Password or the Protection / Fingerprint Recognition for mobile devices.

Don't connect to Public Wi-Fi, use 3G or 4G connections or use VPNs.

Configure that can be Tracked, Remotely wiped or Remotely locked.

Replace devices that are no longer supported by the manufacturers with up-to-date alternatives.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION

ADVOCACY ON DIGITAL SAFETY

BACKING UP YOUR DATA

A better approach !

Take the regular backups of your important data and test that they can be restored.

Test the restoration of data at regular intervals to an alternate device.

Identify what needs to be backed up, i.e. documents, photos, e-mails, contacts and calenders.

Consider backing up to the cloud and you'll also be able to access it from anywhere.

Ensure that the device containing your backup is not permanently connected to any network.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

PREVENTING MALWARE DAMAGE

Avoid unexpected pop-ups , strange e-mails & .exe extension files

Use Antivirus Software on all devices. Install only approved software.

Control all of the access to the removable media. Encourage to transfer files via e-mail or cloud storage instead.

Prevent from downloading third party apps from unknown sources.

Switch on your firewall to create a buffer zone between your network and the internet.

Patch all Software and Firmware by using the 'Automatic Update' option.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

USING PASSWORDS

To protect your data !

Make sure all use encryption products that require a password to boot.

Enforce Password changes at Periodic Intervals.

Switch on the password / PIN protection or the fingerprint recognition for all devices.

Change manufacturers' default passwords on device.

Use Two Factor Authentication (2FA) for banking, e-mail & social media sites.

Provide secure storage and user can reset their own passwords easily.

Avoid using easily predictable passwords (i.e. Family, Pet, First Names, etc).

Use a Password Manager Tool ‘Master Password’ (that provides access to all other passwords)

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

CARRYMINATI'S YOUTUBE CHANNEL (CARRYISLIVE) GOT HACKED

ENABLE TWO - FACTOR AUNTHENTICATION

If their accounts are hacked, yours can be easily hacked too

WHO IS NEXT ?

Follow the steps for two-factor authentication

Settings ⟶ Security ⟶ Two Factor Authentication

Settings ⟶ Security & Login ⟶ Two Factor Authentication

Settings & Privacy ⟶ Accounts ⟶ Security ⟶ Text Message

Settings & Privacy ⟶ Login & Security ⟶ Two Step Verification

Google Account ⟶ Security ⟶ 2 - Step Verification

https://linktr.ee/endnowfoundation

10 INTERNET SAFETY TIPS FOR PARENTS

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

Digital citizenship and internet safety

Don't block all access to technology. Help your child learn to use tech safely and positively.

Take interest in your child's favourite applications or sites. Co-view or co-create at times.

Be the parent. You are in charge. Set boundaries and consider using the filtering software.

Create the family media agreement with tech free zones such as bedrooms, cars, and meals.

Always teach your child what personal informations they should never reveal online (YAPPY acronym).

Help your child learn to filter information online and also navigate fact from fiction.

Navigate digital dilemmas with your child. Avoid using devices as the rewards or punishments.

Balance the Green time and Screen time at home. Focus on the basic developmental needs.

Don't support your child to sign up for sites with the age restrictions (e.g. 15+) if they are underage.

Learn more: Explore reliable resources for parents so you can educate yourself.

https://linktr.ee/endnowfoundation

10 INTERNET SAFETY TIPS FOR KIDS

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

Digital citizenship and internet safety

Laws : Many sites and web tools are 13+. Most images and work online are protected by copyright.

Talk : Tell your parents what you're doing online. Always ask a trusted adult if you're unsure of anything.

Friends : Don't add or meet online friends without parent permission. Do not trust on everything friends tell you.

Privacy : Keep your personal info private : Your full name, address, phone number, your plans, password and your birthday.

Reputation : Do not post anything you wouldn't want teachers, family, friends, and future employers to see.

Question : You can't believe everything you read and see online as there is a lot of incorrect and biased info.

Bullying : Tell someone if you think / see cyberbullying is happening to you or other people you know.

Accounts : Choose some sensible email addresses and usernames and use strong passwords and don't share them with others.

Manners : Be polite and respectful at all times. Treat others online how you'd like to be treated.

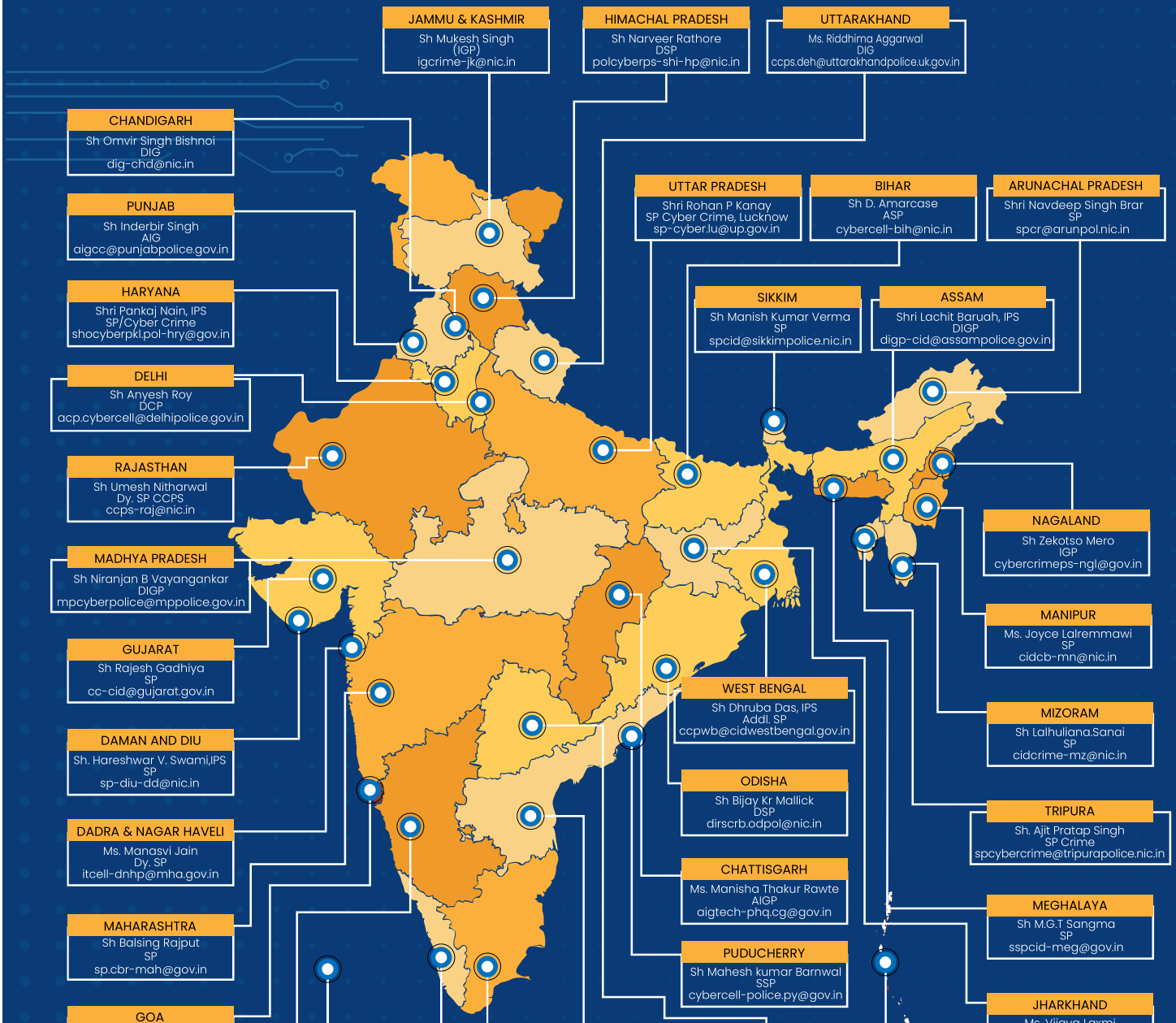
Unplug : Balance your screen time and green time. Get outdoors, move, play, and interact face to face.

https://linktr.ee/endnowfoundation

Nodal Cyber Cell Officers

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

Cyber Crime Reporting Portal
www.cybercrime.gov.in



JAMMU & KASHMIR
Sh Mukesh Singh
(IGP)
igcrime-jk@nic.in

HIMACHAL PRADESH
Sh Narveer Rathore
DSP
polcyberps-shi-hp@nic.in

UTTARAKHAND
Ms. Riddhima Aggarwal
DIG
ccps.deh@uttarakhandpolice.uk.gov.in

CHANDIGARH
Sh Omvir Singh Bishnoi
DIG
dig-chd@nic.in

PUNJAB
Sh Inderbir Singh
AIG
aigcc@punjabpolice.gov.in

HARYANA
Shri Pankaj Nain, IPS
SP/Cyber Crime
shocyberpkl.pol-hry@gov.in

DELHI
Sh Anyesh Roy
DCP
acp.cybercell@delhipolice.gov.in

RAJASTHAN
Sh Umesh Nitharwal
Dy. SP CCPS
ccps-raj@nic.in

MADHYA PRADESH
Sh Niranjan B Vayangankar
DIGP
mpcyberpolice@mppolice.gov.in

GUJARAT
Sh Rajesh Gadhiya
SP
cc-cid@gujarat.gov.in

DAMAN AND DIU
Sh. Hareshwar V. Swami,IPS
SP
sp-diu-dd@nic.in

DADRA & NAGAR HAVELI
Ms. Manasvi Jain
Dy. SP
itcell-dnhp@mha.gov.in

MAHARASHTRA
Sh Balsing Rajput
SP
sp.cbr-mah@gov.in

GOA
Sh Pankaj Kumar Singh
DIGP
picyber@goapolice.gov.in

KARNATAKA
Sh S. Badrinath
Dy. SP
badri@ksp.gov.in

LAKSHADWEEP
Sh Ramdulesh Meena
DSP
lak-sop@nic.in

KERALA
Sh Sreejith
IGP
igpcrimes.pol@kerala.gov.in

UTTAR PRADESH
Shri Rohan P Kanay
SP Cyber Crime, Lucknow
sp-cyber.lu@up.gov.in

BIHAR
Sh D. Amarcase
ASP
cybercell-bih@nic.in

ARUNACHAL PRADESH
Shri Navdeep Singh Brar
SP
spcr@arunpol.nic.in

SIKKIM
Sh Manish Kumar Verma
SP
spcid@sikkimpolice.nic.in

ASSAM
Shri Lachit Baruah, IPS
DIGP
digp-cid@assampolice.gov.in

NAGALAND
Sh Zekotso Mero
IGP
cybercrimeps-ngl@gov.in

MANIPUR
Ms. Joyce Lalremmawi
SP
cidcb-mn@nic.in

WEST BENGAL
Sh Dhruba Das, IPS
Addl. SP
ccpwb@cidwestbengal.gov.in

MIZORAM
Sh Lalhuliana Sanai
SP
cidcrime-mz@nic.in

ODISHA
Sh Bijay Kr Mallick
DSP
dirscrb.odpol@nic.in

TRIPURA
Sh. Ajit Pratap Singh
SP Crime
spcybercrime@tripurapolice.nic.in

CHATTISGARH
Ms. Manisha Thakur Rawte
AIGP
aigtech-phq.cg@gov.in

MEGHALAYA
Sh M.G.T Sangma
SP
sspcid-meg@gov.in

PUDUCHERRY
Sh Mahesh kumar Barnwal
SSP
cybercell-police.py@gov.in

JHARKHAND
Ms. Vijaya Laxmi
SP
cyberps@jhpolice.gov.in

ANDHRA PRADESH
Ms. G. Radhika
SP
cybercrimes-cid@ap.gov.in

TELANGANA
Sh B. Ravi Kumar Reddy
DySP
ccps.cid@tspolice.gov.in

ANDAMAN & NICOBAR
Sh. Madhup Tiwari
IGP
igpint.and@nic.in

TAMIL NADU
Sh G Shashank Sai (for OTHER CYBER CRIMES)
SP
spl-ccdtnpolice@gov.in

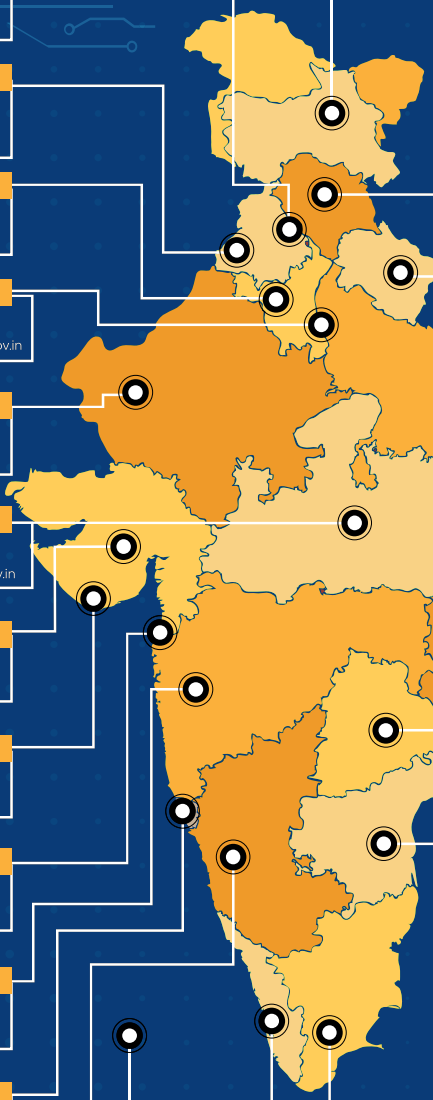
Smt. Jayashree V. (for Women and Children related)
SP
spl-cwctnpolice@gov.in

https://linktr.ee/endnowfoundation

Grievance Officers Cyber Cell

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

Cyber Crime Reporting Portal
www.cybercrime.gov.in



JAMMU & KASHMIR
Sh. B Srinivas
ADGP (0191-2582996)
adgpcidjk@jkpolice.gov.in

HIMACHAL PRADESH
Sh. Sandeep Dhawal
SP (0177-2627955)
sp-cybercr-hp@nic.in

UTTARAKHAND
Sh. Deepam Seth
IGP (0135-2712563)
dgc-police-ua@nic.in

CHANDIGARH
Ms. Nilambari Jagadale
SSP (0172-2760001)
pssput-chd@nic.in

PUNJAB
Sh. Hardial Singh Mann
DIGP (0172-2226258)
aigcc@punjabpolice.gov.in
shocc@punjabpolice.gov.in

UTTAR PRADESH
Dr. Kalluri SP Kumar
ADG(Crime) (0522-2208598)
ccpsstf.gb-up@gov.in

BIHAR
Sh. Shiv Kumar Jha
DIGP (0612-2238098)
dgp-bih@nic.in

ARUNACHAL PRADESH
Sh. Take Ringu
DIGP (0360-2215518)
sit@arunpol.nic.in

HARYANA
Shri Desh Raj Singh, IPS
ADGP(Crime) (01733-253230)
adgp.crime@hry.nic.in

SIKKIM
Sh. Sonam Detchu Bhutia
DySP (03592-204297)
spcid@sikkimpolice.nic.in

ASSAM
Sh. Surendra kumar
IGP (0361-2524494)
igp-cid@assampolice.gov.in

Mr. Prem Nath
Addl.CP (011-20892633)
addlcp.cybertech@delhipolice.gov.in

RAJASTHAN
Sh. Abhijeet Singh
SP SOG (0141-2309547)
singh.kadian@ips.gov.in

NAGALAND
Sh. Renchamo P. Kikon
ADGP (0370-2223897)
renchamo.p@gov.in

MADHYA PRADESH
Smt. Aruna Mohan Rao
SPL DGP (0755-2770248)
spl.dgp-cybercell@mppolice.gov.in

MANIPUR
Sh. Themthing Ngashangva
DIGP (0385-2450573)
themthing.ng@gov.in

GUJARAT
Dr. Shamsher Singh
ADGP (079-23250798)
cc-cid@gujarat.gov.in

WEST BENGAL
Sh. Ashok Kumar Prasad
IGP (033-24791830)
ig2@cidwestbengal.gov.in

MIZORAM
Sh.Balaji Srivastava IPS
DGP (0389-2334682)
polmizo@rediffmail.com

DAMAN AND DIU
Sh. Vikramjit Singh IPS
SP (0260-2250942)
sp-dmn-dd@nic.in

ODISHA
Sh. Madkar Sandeep Sampat
SP (0671-2306071)
splcidcb.orpol@nic.in

TRIPURA
Shri Subrata Chakraborty
AIGP,Crime (0381-2321741)
aigcrime@tripurapolice.nic.in

DADRA & NAGAR HAVELI
Sh. Sharad Bhaskar
SP (0260-2643022)
sp-sil-dnh@nic.in

CHATTISGARH
Sh. R K Vij
SPL DGP (0771-2511623)
vijrk@gov.in

MEGHALAYA
Sh. F G Kharshiing
DIGP (364-2550141)
fg.kharshiing@ips.gov.in

MAHARASHTRA
Sh. Brijesh Singh
SPL IGP/ DGP (022-22160080)
ig.cbr-mah@gov.in

PUDUCHERRY
Sh. Dr. VJ Chandran
DIGP (0413-2231386)
dig.pon@nic.in

JHARKHAND
Sh. Ranjit Prasad
IGP (0651-2490046)
ig-orgcid@jhpolice.gov.in

GOA

Sh. Paramaditya
DIGP (0832-2420883)
digpgoa@goapolice.gov.in

ANDHRA PRADESH
Shri M.Sunil Kumar Naik IPS
DIGP (0863-2340152)
cybercrimes-cid@ap.gov.in

TELANGANA
Smt. Swathi Lakra IPS
ADGP (040-23147604)
igp_wpc@cid.tspolice.gov.in

KARNATAKA
Sh. T D Pawar
DIGP (080-22251817)
digadmincod@ksp.gov.in

LAKSHADWEEP
Sh. Shibesh Singh
SSP (04896-262258)
lak-sop@nic.in

ANDAMAN & NICOBAR
Sh.Deependra Pathak
DGP (03192-230216)
dgp.and@nic.in

KERALA

TAMIL NADU
Shri Shankar K. (FOR OTHER CYBER CRIMES)
IGP (044-28447712)
spl-ccdtnpolice@gov.in

Shri Shankar K. (FOR WOMEN & CHILDREN RELATED)
IGP (044-28447620)
spl-cwctnpolice@gov.in

KERALA
Sh. Dr. Shaik Darvesh
ADGP (0471-2722215)
adgpcrimes.pol@kerala.gov.in

https://linktr.ee/endnowfoundation