CYBER SECURE

A ONE STOP GUIDE TO STAY SAFE ONLINE

An initiative of

SPECIAL BRANCH

In collaboration with

CRIME INVESTIGATION DEPARTMENT

ASSAM POLICE

https://police.assam.gov.in

/police.assam **/assampolice**

"One single vulnerability is
all an attacker needs"

So be alert when you are ONLINE!

CYBER SECURE

https://police.assam.gov.in

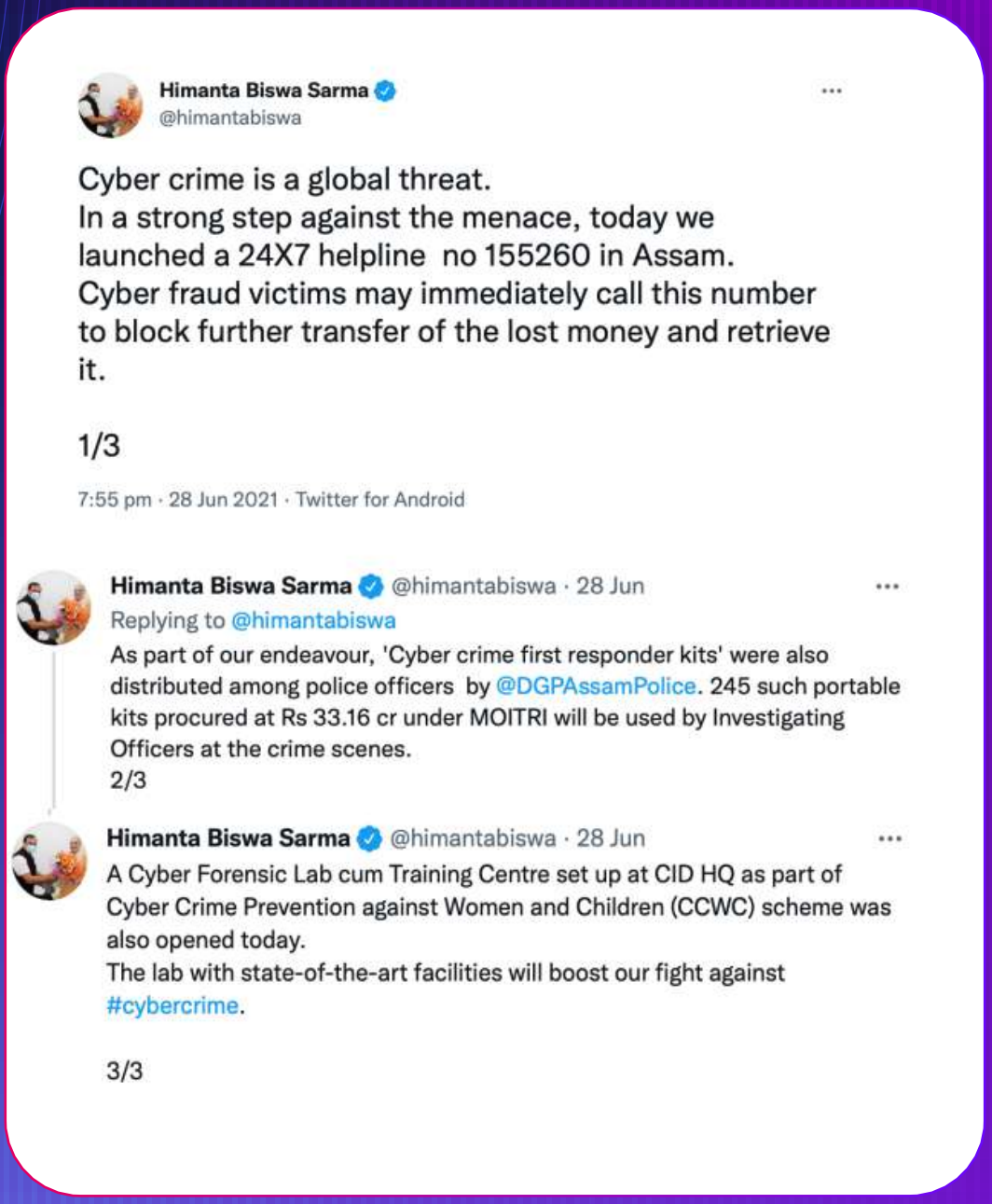
"In the 21st century, where our adversaries are equipped with the latest technologies and techniques of crime both in the real and digital world, the induction of technology-based approach towards investigation and crime resolution in Assam police is the only answer towards the ever-changing threat landscape of the state. Reeling under the shadow of insurgency, illegal immigration, terrorists activities, rising cases of Cyber and digital Crime Assam requires a robust technology induction program in every segments starting from Investigations, Intelligence, Surveillance to fight the crime menace and basically create team of Incident Responders who has Tactical, Operational and Strategic knowledge and visibility to respond to complex challenges in an effective manner and bring in the closure."

Dr. Himanta Biswa Sarma

Chief Minister, Assam

CYBER SECURE

https://police.assam.gov.in



Himanta Biswa Sarma ✓
@himantabiswa

Cyber crime is a global threat.
In a strong step against the menace, today we launched a 24X7 helpline no 155260 in Assam.
Cyber fraud victims may immediately call this number to block further transfer of the lost money and retrieve it.

1/3

7:55 pm · 28 Jun 2021 · Twitter for Android

Himanta Biswa Sarma ✓ @himantabiswa · 28 Jun
Replying to @himantabiswa
As part of our endeavour, 'Cyber crime first responder kits' were also distributed among police officers by @DGPAssamPolice. 245 such portable kits procured at Rs 33.16 cr under MOITRI will be used by Investigating Officers at the crime scenes.
2/3

Himanta Biswa Sarma ✓ @himantabiswa · 28 Jun
A Cyber Forensic Lab cum Training Centre set up at CID HQ as part of Cyber Crime Prevention against Women and Children (CCWC) scheme was also opened today.
The lab with state-of-the-art facilities will boost our fight against #cybercrime.

3/3

Shri Bhaskar Jyoti Mahanta, IPS

Director General of Police, Assam

Foreword

Use of cyberspace for committing crime has been increasing exponentially over the last few years. Cyber attackers use numerous software and codes in cyberspace to commit cybercrime. They exploit the weaknesses in the software and hardware in order to commit crime. In todays world, due to high internet penetration, cyber security is one of the biggest need of the hour as cyber security threats are very dangerous to the country's security. Moreover, as we head into the era of 5th Generation Warfare, know-how of the nuances of cyber security gains irrefutable significance.

It is through awareness among the netizens that cybercrimes can be prevented. It is indeed a commendable initiative of Special Branch of Assam Police that a guide book on how to stay safe online has been compiled which is going to be very helpful in spreading awareness among netizens. The new Assam Police initiatives on training and distribution of cyber forensic kits to 245 numbers of Police Stations in Assam and structural mechanism to counter cyber financial frauds along with other initiatives as a part of I4C initiatives of Govt. of India are being incorporated in this book with the help of state CID. I hope the contents of this guidebook would immensely help Police as well as citizens to remain alert and cybersafe.

Shri Bhaskar Jyoti Mahanta, IPS
Director General of Police, Assam

Shri Niraj Verma, IAS

Principal Secretary,
Home & Political Department, Assam

Foreword

It gives me immense pleasure to know that SB HQRs is going to publish Cyber Awareness Handbook called "Cyber Secure". This will generate awareness among general public about cybercrimes and the necessary preventive measures.

I hope that this publication will be of great help for the general public as it will help them in understanding exactly what cybercrime is, the different types and ways to protect themselves from it.

I wish the publication of Cyber Awareness Book called "Cyber Secure" a grand success.

Shri Niraj Verma, IAS
Principal Secretary,
Home & Political Department, Assam

Shri Hiren Ch Nath, IPS

Additional Director General of Police (Special Branch), Assam

Introduction

In the recent past cybercrimes seem to have proliferated at a rapid pace. It is due to the computer technology that has been implemented in all spheres of human life, which propels everyone to take advantage of such technology for ease of use. In our world today, everyone wants to have a social media account, email account, net-banking account, cloud storage accounts and accounts for online shopping and video streaming services etc. It indicates that we are very much dependent on cyberspace to carry out our day to day life. In such circumstances digital literacy and online social responsibility is the key to thrive on cyberspace. As cyber criminals are coming up with new modus operandi all the time, we have to be updated accordingly. It is worth recalling that in cyberspace a single wrong click of the mouse can ruin everything, from huge monetary loss to severe damage in public and personal life.

In this context, the Special Branch Headquarters of Assam Police has nurtured the idea of publishing a handbook named as "Cyber Secure – A one stop guide to stay safe online", which would certainly create awareness among public at large.

I would like to gratefully acknowledge the guidance of Shri Bhaskar Jyoti Mahanta, IPS, DGP Assam, Shri Gyanendra Pratap Singh, IPS, Special DGP (L&O) and Shri A. Y. V. Krishna, IPS, ADGP (CID) in the journey of this new endeavour.

I also acknowledge the hard work of Shri Padmanabh Baruah, IPS, Smt Papori Chetia, APS, Shri Ruhul Amin, AHGS and End Now Foundation editorial team to make the concept into a reality.

I wish that this very first edition of "Cyber Secure" will enormously help citizens, students community, Govt. servants, investigators and security consultants.

Shri Hiren Ch Nath, IPS

Additional Director General of Police, (Special Branch) Assam

Editorial Team:

Shri Hiren Ch Nath, IPS – Concept & Ideation
Shri Padmanabh Baruah, IPS – Concept & Coordination
Smti Papori Chetia, APS – Coordination
Shri Ruhul Amin, AHGS – Data Review & Compilation
Shri Dipankar Boro, Inspector (UB) – Data Review & Compilation

Shri Anil Rachamalla, End Now Foundation – Research & Ideation
Shri Macherla Vijay Kumar, End Now Foundation – Designer

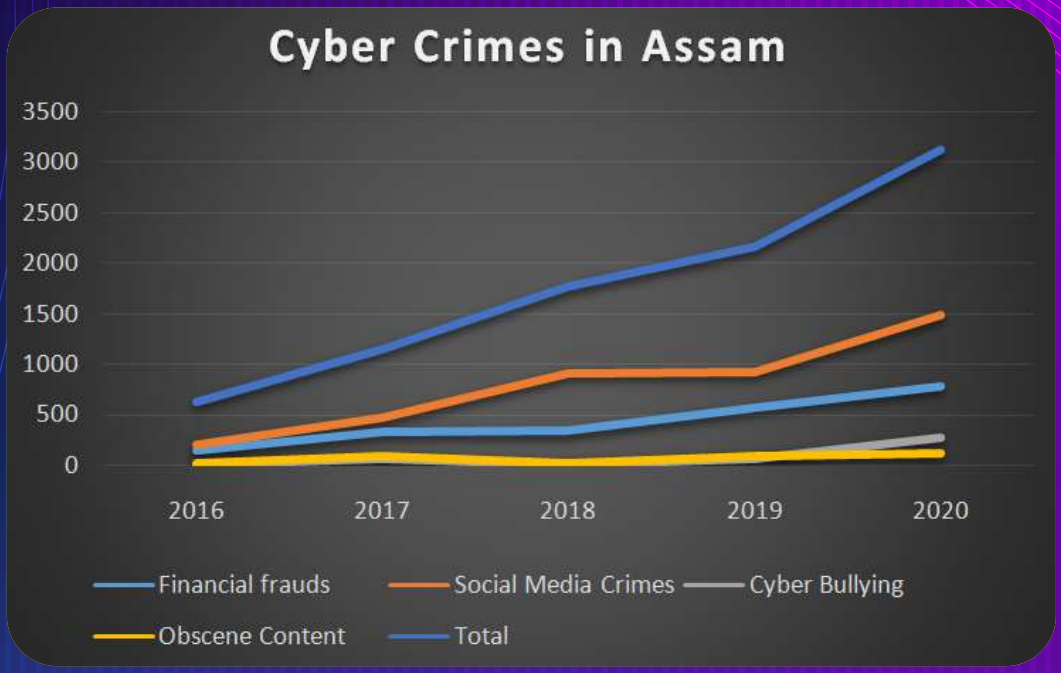
Table of Contents

CYBERSPACE IS NOT SO SAFE ANYMORE

CYBER SECURE

https://police.assam.gov.in

HOW VULNERABLE ARE YOU ?



India ranks 3rd among nations facing most cyber threats: Symantec

The United States led the pack, followed by China at the second spot, according to the company's Internet security threat report (ISTR).

India ranked third in the list of countries where the highest number of cyber threats were detected, and second in terms of targeted attacks in 2017, according to security software firm Symantec.

"India is ranked third among list of countries globally where most of the threats were detected and it is second in terms of targeted attacks," Tarun Kaura, Director, Enterprise Security Product Management, Asia Pacific and Japan, Symantec said.

The United States led the pack, followed by China at the second spot, according to the company's Internet security threat report (ISTR).

COMMON CYBER THREATS

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.

CYBER SECURE

PHISHING ATTACK ALERT

Gear up to protect yourself from cyber criminals.

Dear,
SBI.. CUSTOMER YOUR SBI.. SAVING ACCOUNT & DEBIT CARD WILL BE SUSPENDED ON 19/10/2019 BECAUSE DUE TO INCOMPLETE KYC.. IN YOUR BANK ACCOUNT TO REACTIVATE YOUR SAVINGS ACCOUNT KINDLY PLEASE UPDATE YOUR FULL KYC.. IN YOUR BANK ACCOUNT BY VISITING THE LINK BELOW https://docs.google.com/forms/d/e/1FAIpQLScNGiiu2Go9r7se21LaMHNCPRjpE6eLUHuVYecVIBeaScBI2Q/viewform

Sample Phishing SMS

HOW TO STAY PROTECTED

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.)

*****I

The sender doesn't address you by name.

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

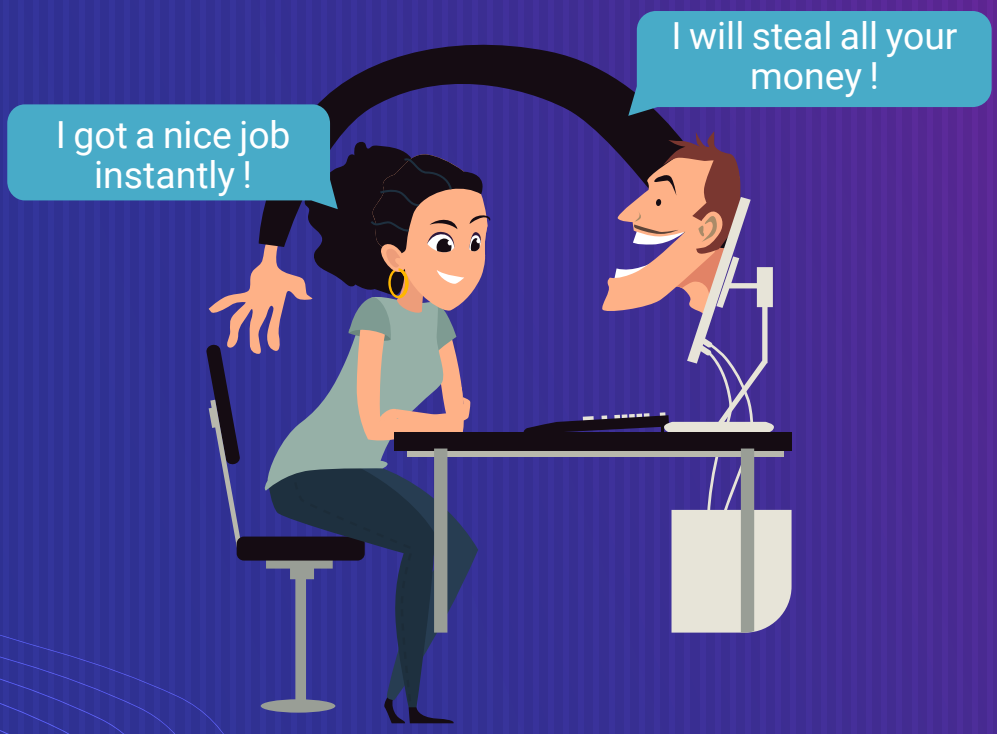
When in doubt, always contact a Technical Expert for help.

CYBER SECURE

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 instant messaging platforms.
- Vague job requirement and job description.
- Search results about the Company or the job don'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



CARD FRAUD !

Always guard your Cards and the Card details.

Do not let your Card out of your sight when making a transaction.

Ask the retailer to confirm the amount being debited from your Card.

Sign the new cards as soon as they arrive.

Check your receipts against your Online Statements.

Carefully discard your receipts from Card transactions and the information related to your financial affairs.

Don't leave your cards Unattended in a Public Place. Keep personal belongings with you at all time.

Never write down your PIN nor disclose to anyone.

When making Online transactions make sure you are using Updated Antivirus & Operating System Software.

Only buy from trusted sources. For Internet purchases, use the Security Protocol 3D - Secure.

When replacement card arrive, cut expired / unused / blocked cards into several pieces, inluding through the magnetic strip and / or chip.

CASH MACHINES (ATMs)

Always try to be aware of others around you.

Don't use the ATM if there are any signs of tampering.

If the ATM does not return your Card,then report it to your Bank.

Shield your PIN.

PAYMENT TERMINALS (POS)

Card - skimming can also occur at the retail outlets, particularly bars, restaurant areas, the parking ticket machines & the (unnamed) petrol stations.

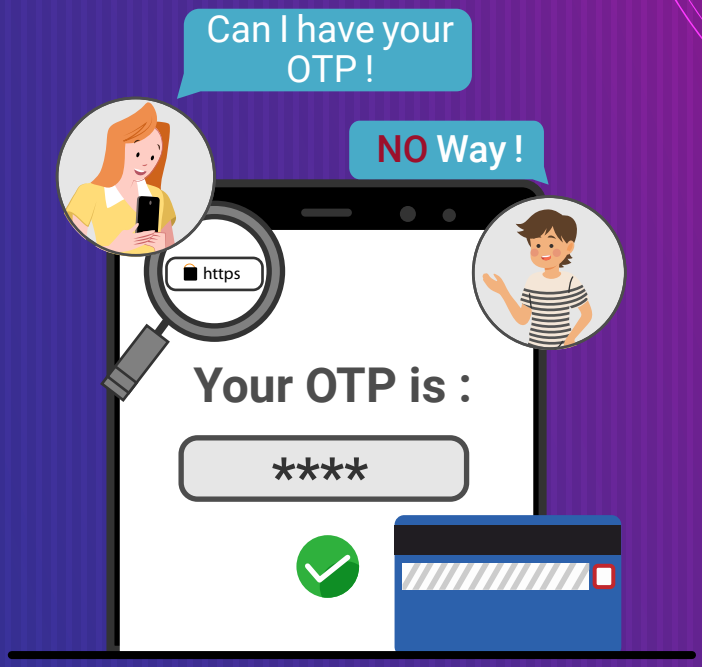
Never lose sight (and if possible, touch) of ATM card during the payment transactions.

Insist that your card is visible to you at all times.

CYBER SECURE

HOW THE 'KYC' SCAM WORKS

1. You get a call that your wallet or bank KYC is invalid.
2. Caller says it can be validated online so that your account is active again.
3. You are asked to download an app to facilitate step-by-step guidance.
4. When you use the app, caller can see your phone screen.
5. He asks you to transfer a small token amount to your wallet.
6. He uses them simultaneously to transfer larger amounts from your bank.
7. When you do so, he can see your password and other details.
8. Victim gets OTPs for all transfer requests but these can be seen by scamster via the app.
9. In a matter of minutes, the scamster cleans out the bank account.



GUARD THAT OTP

Your One-Time Password (OTP) can be used to steal money from your bank account. Refrain from sharing it to stay out of trouble.

- Never share your One Time Password (OTP).
- Keep Changing Your ATM PIN frequently.
- Never share your CVV.
- Check for https:// and the Lock Icon for Secure Online Transaction.
- Never save Credit / Debit Card details on e-Commerce websites.

CYBER SECURE

THINK BEFORE YOU ENTER YOUR

SAY NO TO

- Advance Payments.
- Sharing Personal Details,
  PIN Number, OTP, CVV, Account Number, etc.
- Transferring, receiving money while on call.

Your PIN is NOT required when RECEIVING UPI Payments via

Paytm | PhonePe | G Pay

BEWARE: Payments through Online Platforms are Robust but Susceptible to Fraud.

99% of Payments are Prone to Phishing and Social Engineering Crimes.

CYBER SECURE

HOW DEBIT/CREDIT CARD SKIMMING WORKS

Here are some of the ways that thieves use to steal bank information from atms :

Fraudsters switch the entire device.

Fraudsters install a Skimmer.

Fraudsters install a new keypad.

Fraudsters install a camera.

HOW TO PROTECT YOURSELF

- ATMs at banks may be safer than those at gas stations and stores.
- Jiggle the card as you withdraw it from the slot, it might loose a card skimmer.
- As you enter your PIN, cover the keypad with your other hand.
- Don't use an ATM or payment machine if it appers altered.
- If having trouble using an ATM, don't accept help from strangers.
- Check your bank statements regularly to see any suspicious activity.

WHAT IS SIM SWAP FRAUD?

STEP 1

Fraudsters gather a customer's personal information through Phishing, Vishing, Smishing or any other means.

STEP 2

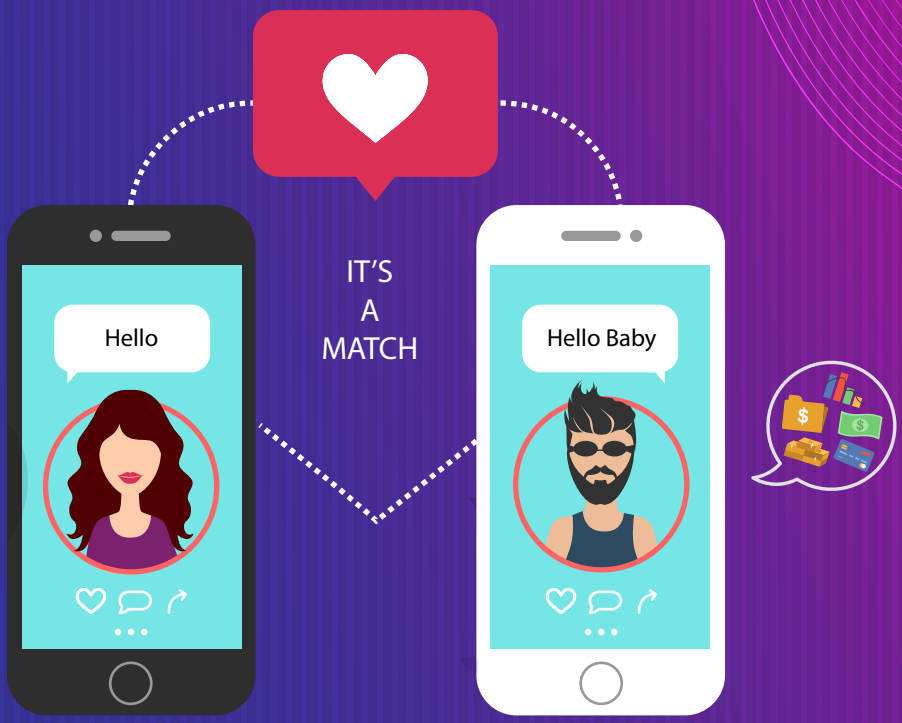
They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the fake ID proof posing as the customer.

STEP 3

The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.

STEP 4

Fraudster then generates a One Time Password (OTP) required to facilitate transactions, using the stolen banking information. This OTP is received on the new SIM held by the fraudster.



AVOID FALLING PREY TO ROMANCE FRAUD

- Do not indulge in online chatting, dating or get emotionally involved with people without verifying the truthfulness of clients.
- Never spend money or share your details to strangers/social media friends.
- Online follower asks to communicate outside the dating website/platform only after a few contacts or conversations.
- Do a www.tineye.com or Google Reverse Image Check of your fan to help determine if they really are who they say.
- No sharing of intimate pictures or videos online. Scammers are known to blackmail their targets using past shared pictures or videos of you that you don't want others to see.

NOTHING COMES FREE

THE TIMES OF INDIA

CITY

City | Bengaluru | Mumbai | Delhi | Hyderabad | Kolkata | Chennai | Agartala | Agra | Ajmer | Amaravati | Ahmeda

Crime | Civic Issues | Politics | Schools & Colleges | Karnataka Elections | Citizen Reporter | Photo

NEWS / CITY NEWS / BENGALURU NEWS / MAN LOSES 6 LAKH IN MATRIMONIAL FRAUD IN BENGALURU

TOP SEARCHES: Karnataka news | Karnataka Corona Cases | Karnataka lockdown guidelines | Royal Challenge

Man loses 6 lakh in matrimonial fraud in Bengaluru

TNN | Updated: Feb 24, 2021, 08:05 IST

A- A+

PREVENT MATRIMONIAL FRAUDS

How to prevent yourself from being a victim of matrimonial fraud :

- Do a thorough Profile Check.
- Always look for 'Verified' Profile Matches on Marriage Portal.
- Never give money to anyone.
- Never reveal your portal account information.
- Stay informed while meeting in person.
- Stay informed while signing on any document.

BEWARE OF LOAN FRAUD

WARNING SIGNS

- No credit check required.
- Lender is not registered with the Government legally.
- No physical address.
- Advance payment.
- Offer expires in a few days.

SAFETY TIPS

- Look for a secure Payment (https:// URL with a Pad Lock Symbol).
- Never share OTP/PIN numbers to the buyer or seller.
- Never do the payment while you are on the call.
- Do not click and fill up any Short Links provided by the buyer or seller.
- Do no fill out google form links provided by the buyer or seller.
- Do not scan the QR code.
- Never pay any advance for loans.

GUARD YOURSELF AGAINST LOTTERY FRAUD

FEW FRAUDS

- Kaun Banega Crorepati
- Scratch Card Gift
- RBI Lottery
- European Lottery

SAFETY TIPS

- Never click on Short Links sent through e-mail/SMS.
- Click on Websites that start with https://.
- There is an attachment that you were not expecting.
- Sender doesn't address you by name.
- You don't need to pay any money in advance to win a lottery.
- We cannot win money in a lottery or competition unless we have purchased or participated personally.
- Competitions and lotteries do not require you to pay advance fee to collect winnings.
- Never transfer funds to an unknown person or entities in anticipation of high returns.

STAY SECURE FROM IDENTITY FRAUD

How to safeguard yourself from being an identity victim :

- Do not open short links that have been sent via e-mail or SMS.
- Don't Update Antivirus software both on PC and Mobile phone.
- Don't communicate about financial / password information on e-mail or SMS.
- Do not post Date of Birth, place of birth or e-mail address or Mailing Address on Social Media Platforms.
- Change Passwords periodically.
- Don't use the 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.

CYBER SECURE

TIPS TO PROTECT FROM CYBER FRAUDS

CYBER SECURE

CYBER SAFETY

How to stay safe online

Always keep your information & the passwords private

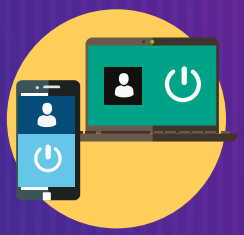
Be careful of what you are posting online

Always check your privacy settings

Shop safely on the trusted websites

Choose strong passwords

Protect all of your devices with an antivirus Software



Remember to log off

Check the website url

Always check the subject of an e-mail before you open it

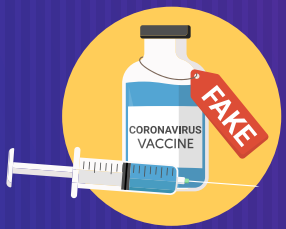
Avoid phishing & other scams

Always keep your children safe online

Respect yourself & others online

Avoid Online Dating Sites

Avoid Insurance Fraud



Avoid Vaccine Fraud

Avoid Bitcoin Fraud

CYBER SECURE

USING PASSWORDS

To protect your data !

Make sure you 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)

SOCIAL MEDIA IS A LOT MORE FUN WHEN YOU PAY ATTENTION TO SAFETY

Here are some tips to stay safe in the cyberworld

- Use a strong password.
- Use a different password for each of your social media accounts.
- Set up your security answers (this option is available in most social media platforms).
- Access social media from a computer.
- Be cautious while accepting friend requests.
- Click on Links with caution.
- Be careful about the personal information you share.
- Become familiar with the privacy policies of the social media channels.
- Protect your computer by installing antivirus software.
- Remember to log off when you are done.

CYBER BULLYING

TYPES

Cyber Stalking

Repeatedly sending the messages that include threats of harm or are highly intimidating.

Impersonation

Pretending to be someone else & sending or posting any material online that makes that person look bad, gets that person in trouble.

Denigration

Dissing someone online. Sending or posting any cruel gossip about a person to damage his or her reputation or friendship.

Harassment

Repeatedly sending some offensive, rude, and insulting messages.

Outing & trickery

Sharing someone's secret or embarrassing information online.

Flaming

Online fights using electronic messages with angry and vulgar language.

Exclusion

Intentionally excluding someone from online group, like a 'buddy list'.

CYBER BULLYING

AFTER EFFECTS

Health issues

Suicide

Depression

Bankruptcy

Alcohol

Violent

CYBER SECURE

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 software 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.

CYBER SECURE

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.

Enable 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 your smart phone, such that it can be Tracked, Remotely wiped or Remotely locked.

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

CYBER SECURE

BACKING UP YOUR DATA

A better approach !

Take 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.

CYBER SECURE

PREVENTING MALWARE DAMAGE

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

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

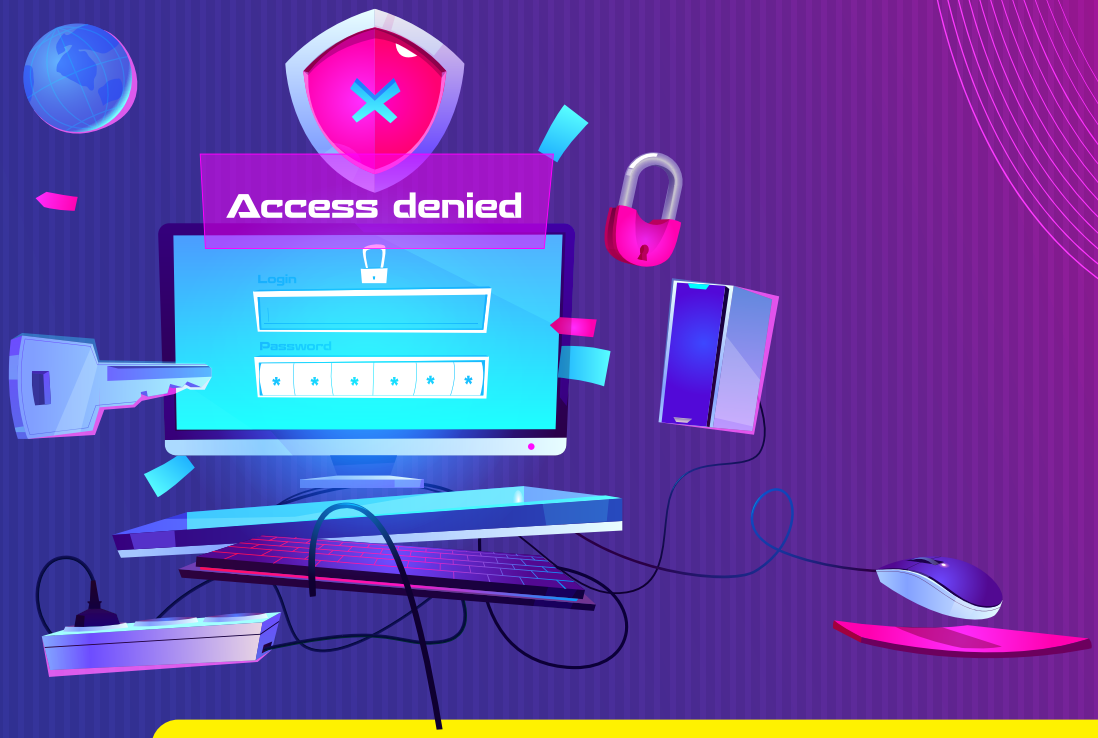
Control all of the access to the removable media. Encourage to transfer files via e-mail or cloud storage instead.

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.

CYBER SECURE



ENABLE TWO - FACTOR AUTHENTICATION

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

CARRYISLIVE

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

CYBER SECURE

10 INTERNET SAFETY TIPS FOR PARENTS

Digital citizenship and internet safety

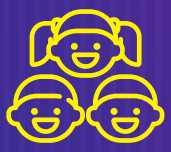
Don't block all access to technology. Help your child learn to use tech safely and positively.

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).

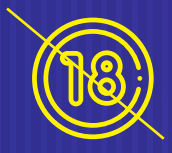


Help your child learn to filter information online and also navigate fact from fiction.

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.

CYBER SECURE

10 INTERNET SAFETY TIPS FOR KIDS

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 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.

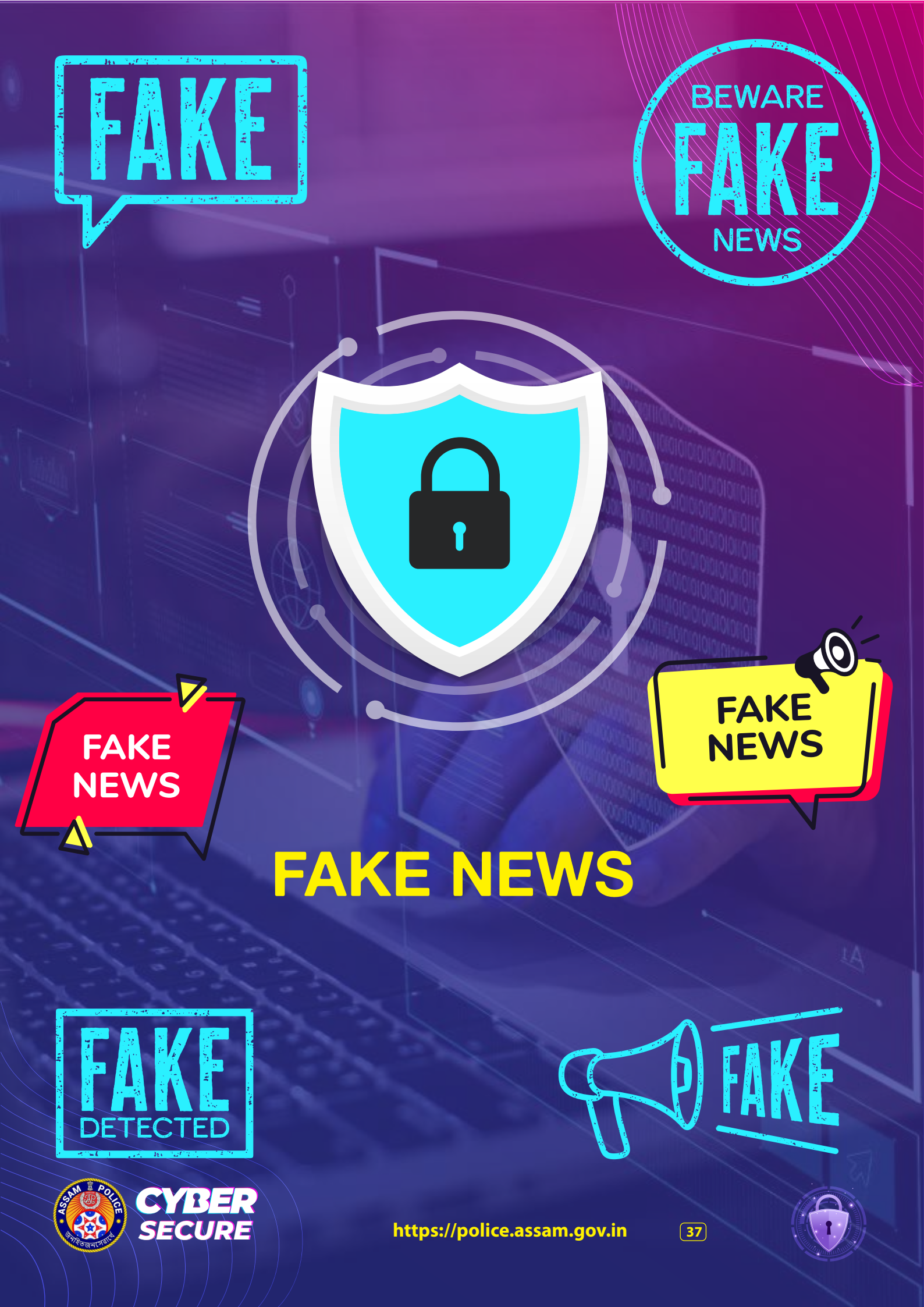
Bullying : Tell someone if you think / see cyberbullying is happening to you or other people you know.

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.

CYBER SECURE


FAKE
BEWARE
FAKE
NEWS
FAKE
NEWS
FAKE
NEWS
FAKE NEWS
FAKE
DETECTED
FAKE
CYBER
SECURE

PEOPLE ARE MISUSING SOCIAL MEDIA, MESSAGING AND INTERNET TO SPREAD FAKE NEWS

Here are ways how you can spot fake news.

- Check the source and URL.
- Refer fact checking sites (www.factly.in).
- Read beyond the headline.
- Check if it's a joke.
- Check the date.
- Check your biases before judgement.
- Watch for any unusual formatting.
- Do Google Reverse Image Check.

SPOTTING FAKE NEWS ON SOCIAL MEDIA & INTERNET !

Consider the source

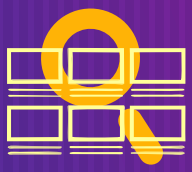
Is the source credible, trustworthy and well known? Consider the source that is from a reputed news paper, news channel or online news website.

Check the url

Does it seem legitimate? Does the website have a track record of being reliable? Many sites use similar sites ending with .io .co .com.

Who's the author?

Did you search for the author's name online to see if they are credible & very well respected? Many fake sites won't use the author's name.



Read beyond headline

Does the article seem balanced, fair & objective? Always study it critically, detecting the tone & viewpoint while checking your bias at the door.

Disregard your bias

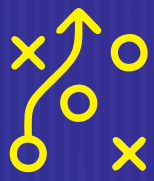
It is easier to believe stories that confirm your internal views. But the next time you see on social media post that flames your political, racial or religious views.

Get a second opinion

If a story makes you very angry and a dig deeper, consult known contact or use debunking sites before forwarding.

SPOTTING FAKE NEWS

9 TYPES OF MIS AND DISINFORMATION

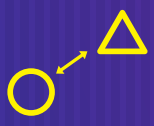


False Connection
When the headlines, visuals or the captions do not support the content.

False Context
When the genuine content is shared with the false contextual information.

Manipulated Content
When some of genuine information or the imagery is manipulated to deceive.

Satire or Parody
No intention to cause harm but has potential to fool.



Misleading Content
Misleading the use of information to frame an issue or individual.

Imposter Content
When genuine sources are impersonated.

Fabricated Content
Content that is 100% false, and designed to deceive and do harm.

Propaganda
When content is used to manage attitudes, values and knowledge.

Sponsored Content
Advertising or PR is disguised as editorial

SPOTTING FAKE NEWS
PHOTO VERIFICATION

Identify and verify the original source and the content (which includes location, date and the approximate time).

Always use tools like FotoForensics/Findexif for the information on camera model/timestamp.

Try to find multiple sources. Challenge the original source to prove veracity - ask follow up questions.

Using Wolfram Alpha, check if the weather captured in photo (e.g. sunny, rainy, overcast) was actually the weather in that area.

Always use tools like www.tineye.com and https://images.google.com on Google.

SPOTTING FAKE NEWS
VIDEO VERIFICATION

Identify and verify the original source and the content (which includes location, date and the approximate time).

Try to find some multiple sources. Challenge the original source to prove veracity - ask follow up questions.

Use the Amnesty International's Data Viewer.(https://citizenevidence.amnestyusa.org).

Scrutinize uploader's name and the date of upload.

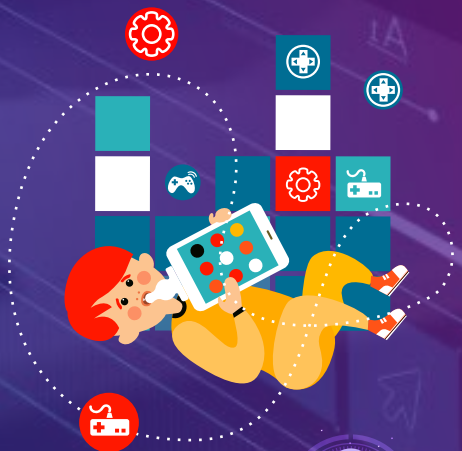
What information does the social media / affiliated accounts give that indicate location, activity, reliability, bias or agenda of uploader?

How long have these accounts been active? How active are they?

Is the person listed in online databases or the networking platforms e.g. Linkedln?

Are the other accounts, including social media, a blog or website - affiliated with the uploader?

DIGITAL DETOX?



CYBER SECURE

SMARTPHONES

THE BIGGEST NON - DRUG ADDICTION OF THE 21ST CENTURY

If your smartphone has made you it's slave,
Here's a step - by - step approach to detach from it

- Disable notifications on your smartphone.
- Keep your phone away during meals with your friends and family.
- Charge your device outside the bedroom.
- Device - free meetings.
- Access social media from your computer instead of your smartphone.
- Use grey scale mode on your phone.
- Keep only the most important tools on your home screen.
- Screen time for IOS and digital wellbeing for android to control the technology usage.

ONLINE GAMING IS PUBGECTED TO A LOTS OF RISKS

Read on to know it's negative consequences.

- All day addiction to games.
- Bad influence on health.
- Isolation from family & friends.
- Waste of precious time.
- Face a problem of insomnia.
- An expensive hobby.
- Rising level of aggression.
- Affects the eyesight.

HOW EXPOSURE TO BLUE LIGHT AFFECTS YOUR BRAIN AND BODY

By disrupting melatonin, smartphone light ruins sleep schedules. This leads to all kinds of health problems:

The disruption to your sleep schedule might leave you distracted and also impair your Memory the next day.

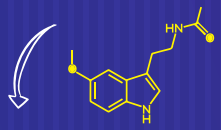
There's some evidence that blue light could damage our vision by harming the Retina over time — though some more research is needed.

A poor night's sleep caused by smartphone light can make it harder to learn.

Researchers are investigating whether or not blue light could lead to Cataracts.

Over the long term, not getting enough sleep can lead to Neurotoxin buildup that makes it even harder for you to get good sleep.

There is a connection between light exposure at night and the disturbed sleep that comes with it and an increased risk of breast and prostate Cancers.



People whose melatonin levels are suppressed and whose body clocks are thrown off by light exposure are more prone to Depression.

By disrupting melatonin and sleep, smartphone light can also mess with the hormones that can control hunger and potentially increasing Obesity Risk.

GUIDE TO STAY SAFE ONLINE

KEY LOGGER:

Always check Mouse/Keyboard cable, if you are accessing your valuable information through internet using any device/PC kept for public use. Cyber criminals might connect hardware key logger to steal the information(s) and use it for duping people. Public devices might have key loggers installed which are specially designed to capture input from keyboards which enables the fraudsters to have access to information most importantly username & password.

Tips for Safety :

*Prefer virtual keyboards while logging in specially if you need to access net banking facility from a public computer/cyber café or a shared computer.
*Please delete the browsing data after completion of online session and see the 'lock' icon on the status bar of the browser while visiting the bank site or during online transaction.

FASTAG FRAUD:

Fraudsters are cheating people in the name of helping them to register or activate their wallets for FASTag as it has been made mandatory for all commercial and private vehicles from 15th January, 2020. As FASTag is based on RFID, FASTag chips can be cloned and misused. There is also a possibility of copying FASTag data-on-air by various devices.

Tips for Safety :

*Buy FASTags from approved agencies and never entertain any calls/messages asking for FASTags support.
*Install genuine applications provided by NHAI. My FASTag application available on Google Playstore has been launched by NHAI under Indian Highways Management Company Ltd. (IHMCL)

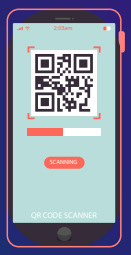
DARKGATE:

It is a malware which has both ransomware and crypto mining components. DarkGate is capable of stealing crypto wallets enabling remote control of the system, perform keylogging, evade antivirus detection installing ransomware and cryptocurrency.

It uses 'torrent files' which claim to be of popular movies or television series but actually encoded Visual Basic Scripts (.vbe files).
DarkGate is a spam e-mail claiming to be a failed delivery notification. The e-mail contains a malicious attachment sent by another encoded Visual Basic Script File claiming to be a torrent.

Tips for Safety:

*Avoid clicking on links and attachments in email as most of the infections are primarily induced via phishing emails, malicious advertisements on websites and third party apps and programs.
*Take regular back up of data as in the event of attack, it is the only way to recover lost data.
*Avoid applying updates/patches from any unknown/unofficial sources.



SCAM THROUGH QR SCAN:

Be cautious while scanning any QR codes using payment apps. QR codes have embedded account details in them to transfer amount to particular account. Con artists use QR codes to automatically launch payment apps or follow a malicious social media account.

Tips for Safety:

*Please don't trust any QR code that was mailed to you or that appeared in a text, online post.
*Avoid using QR code to pay any bill.
*Consider adding protection that checks for malicious or inappropriate content.
*Some Anti Virus companies have QR scanner apps that check the safety of a scanned link before opening.

JUICE JACKING:

Always avoid using public / unknown charging ports / cables. In public places like shopping malls, stations etc, there are public charging points to which one can recharge their mobile phone(s), laptop(s) and other devices. It is the most common type of cyber attack where the charging port doubles as a data connection over USB and involves either installing malware or surreptitiously copying/stealing personal data/sensitive information from the connected electronic device. It is a kind of security exploit which takes advantage of the fact that the particular device's power supply passes over the same USB cable the connected device uses to sync data.

Tips for Safety:

*The most common way to protect your device from Juice Jacking is to avoid using chargers that are left plugged into wall sockets.
*Install any Anti-Virus solution preferably one that costs and not which is freely available on net or opensource. Its installation in the device prohibits data theft.

FRAUDS BY COMPROMISING CREDENTIALS ON RESULTS THROUGH SEARCH ENGINES:

Avoid searching for customer care contact details on search engine. These are often camouflaged by fraudsters. One should always look for official websites of Banks / companies/e-commerce to get contact details rather than clicking on any suspicious links.

Tips for Safety:

*Avoid searching any customer care number on Google. Random Google searches might take you to any fake call centre resulting in financial loss.

DO'S & DON'TS FOR WHATSAPP USERS:

DO'S

- Do not post fake news, hate speech or information in groups.
- Do not forward or circulate any such news you get from other members of the group.
- Immediately delete any post, if you find it objectionable or if the admin notifies you.
- Check the source and veracity of any news/image/video/meme you receive, before posting it on the group.
- If you find any piece of information, fake news or hate speech, report it on www.cyber crime.gov.in or to your nearest PS and also inform your group admin immediately.
- Never share any content that is violent, pornographic and discriminative against any religion/community.

DON'TS

- Ensure that every group member is reliable and responsible enough to share only verified news.
- Inform all the group members about the rules of posting in the group.
- Warn all the members and prevent them from sharing objectionable content.
- Actively and regularly monitor content that is being shared on the group.
- It is advisable that if the group is uncontrollable, then the group settings can be changed to only where admins have the right to post.
- Inform the police if any member(s) resort to mischief and share objectionable content.

CYBER-CRIMES AND THE LAW

CYBER CRIMES & LAW

S.No	Category of Offences			Sec of Law–Applicability	Description Of the Offence
	Major Head	Minor Head	Sub-Head		
1	Identify Theft Sec.66(C), 66 (D) ITAct,420 IPC.	Bank Related Frauds: Vishing (Call) Fraud Smishing (SMS) Fraud Phishing (e-mail) Fraud	Aadhaar Linkage PAN Card Linkage KYC updation- Blocking of card Card limit enhancemet Reward Points	66(C)IT Act and 420IPC	A.Calling over phone pretending as bank representatives,collection of bank A/c credentials like Card etails,OTP and misusing the same. B.SendingSMS/e-mail to the victim, collection of credentials of bankA/c, Card details,OTP and misuse of the same.
			Replacement of card -with photo/Chip Any Others		
		Skimming/ Cloning of Cards etc.	ATM Center Merchant Place	66(C) IT Act and 420 IPC	Placing Skimmers at ATM Centers / collecting data at Merchant Places.With-drawal of amounts with cloned cards from ATM's and from Merchant Places.
		Fake Customer Care Service Fraud	Google Just Dial Any Others	66(C), 66(D) IT Act and 420IPC	Posting fake customer care service Ads in Google, Just Dial etc.,in the name of original-firms/companies and deceiving the victims in the name of fake Customer Care Services etc. and taking huge amounts.
		Income TaxFraud		66(C) ITAct and 420 IPC	Personating as if from Income Tax department and cheating the victims on the pre text of better return of tax paid amount etc.
		SIM SWAP Fraud		66(C) & (D)IT Act and 420IPC	Submitting forged documents and collecting replace SIM cards from stores of TSP's for committing bank Frauds.

CYBER CRIMES & LAW

S.No	Category of Offences			Sec of Law–Applicability	Description Of the Offence
	Major Head	Minor Head	Sub-Head		
		Job Fraud, Visa Fraud	Naukri Shine Monster Any Other	66 (D) IT Act and 420 IPC	Calls / Messages / e-mails are made / sent to the victims on the pretext of arranging Job / Visa etc., and deceiving them by parting with money towards Registration fee, advance fee etc.,
2	Online Frauds Sec. 66 (D) IT Act, 420 IPC.	Loan Fraud		66 (D) IT Act and 420 IPC	Personating as financial institutions and deceiving the victims on the pretext of arranging loans at low rate of interest etc.,
		Insurance Fraud		66 (D) IT Act and 420 IPC	Personating as insurance company representatives and deceiving the victims on the pretext of better insurance plans etc.,
		Lottery Fraud		66 (D) IT Act and 420 IPC	Either calling or sent SMS / e-mails to victims by mentioning that they have won prize over lotteries organized by popular organizations and thus deceiving victims to part with money on the pretext of paying for advance fee, getting no objection
		Advertisement Portal Fraud	OLX & Quikr CarDekho Facebook Instagram Any Other	66 (D) IT Act and 420 IPC	Posting fictitious / fake Ads in classifieds of Social Media Platforms and deceiving the victims.
		Gift Fraud (By using the	Snapdeal Shopclues Amazon Flipkart Clubfactory Naaptol Home Shop 18 Any Other	66 (D) IT Act and 420 IPC	Securing customer data of e-commerce platforms and deceiving the customers on the pretext of winning Gift.

CYBER CRIMES & LAW

S.No	Category of Offences			Sec of Law–Applicability	Description Of the Offence
	Major Head	Minor Head	Sub-Head		
		Trading Fraud	Share Trade Forex Trade Commodity Trade Investment Advisors	66 (D) IT Act and 420 IPC	Cheating the victims on the pretext of fetching huge amounts on investing amounts in Share / Forex / Commodity Trade / by paying amounts towards Share market Tips (IA's).
		Delivery of duplicate / Sub-standard products Fraud		66 (D) IT Act and 420 IPC	Cheating the victims by sending duplicate / Substandard articles to the victims instead of sending the original products shown in online
		Mobile Fancy Number Fraud		66 (D) IT Act and 420 IPC	Delivery of duplicate / Sub-standard products Fraud
		Cell Tower Installation Fraud		66 (D) IT Act and 420 IPC	Personating cell companies and cheating the victims in the name of agreement with TSPs & victims and thereby parting with amounts in the name if advance fee, security deposit etc.
		Online relationship Fraud	Friendship through A). Matrimonial – Websites B). Social Media Platforms	66 (D) IT Act and 420 IPC	Posting attractive fake profiles over matrimonial websites / Social Media platforms once victims get attracted to such posts and after gaining faith collecting money on false pretexts.
		Dating / Female escort Fraud		66 (D) IT Act and 420 IPC	Cheating in the pretext of supply of raw materials, better returns in short term etc.
		Business and Investment Fraud		Business and Investment Fraud	Cheating in the pretext of supply of raw materials, better returns in short term etc.

CYBER CRIMES & LAW

S.No	Category of Offences			Sec of Law–Applicability	Description Of the Offence
	Major Head	Minor Head	Sub-Head		
3	Cyber Stalking Sec. 354 (D), 509, 506, 507 IPC and Sec.67 of IT Act.	Stalking over 1. Social Media, 2. Classified Websites 3. Pornographic Websites.	Facebook Instagram Dating Websites Porn Websites Any Other	354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable.	Creating fake profile in the name and identities of victim / sending add friend requests to victim friends, posting the mobile numbers of victim in Classified / Pornographic Websites etc.
		Stalking over 1. SMS 2. e-mails 3. WhatsApp (VOIP etc.)		354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable	Sending unsolicited e-mails and messages with abusive or objectionable contents.
		Stalking by fake Social Media Profiles.		354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable.	Creation of fake profile over Social Media.
		Blackmailing, Intimidation, Sextortion.		354 (D), 506 / 507, 509 IPC and 384 IPC, if	Creating fake profile in the name and identities of victim / sending add friend requests to the victim friends coupled with demand for ransom.
4	Violation of Privacy Sec.66(E) IT Act, 354 (C) IPC.	Taking images through phones.		66-E IT Act, 354 -C IPC (Depending on the case)	Taking images of private parts and activities of people over mobiles phones etc.
	Sec.66(E) IT Act, 354 (C) IPC.	Taking photos with hidden cameras.		66-E IT Act, 354 -C IPC (Depending on the case)	Keeping hidden cameras and capturing images of private parts at bathrooms, trial rooms etc.,
5	Cyber Pornography Sec.67, 67 (A) IT Act.	Circulation of obscene images / text.		67 and 67-A IT Act	Cheating in the pretext of supply of raw materials, better returns in short term etc.,
		Circulation of Obscene videos.		67 and 67-A IT Act	Circulation of obscene videos over Social Media, emails or WhatsApp.

CYBER CRIMES & LAW

S.No	Category of Offences			Sec of Law–Applicability	Description Of the Offence
	Major Head	Minor Head	Sub-Head		
6	Child Pornography Sec.67, 67 (B) IT Act, POCSO Act.	Circulation of Obscene child porno		67, 67 (B) IT Act and POCSO Act	Circulation of obscene videos related children over social media, e-mails or WhatsApp or downloading child sexual porno, enticing children for online relationship etc.
7	Source Code Tampering Sec.65 IT Act	Stealing, deletion and destruction of source code		354 (D), 509 IPC, if the content is obscene Sec. 67 of IT Act is also applicable	Stealing of computer programme / application/ code and making use of self or for others.
8	General Computer Offences Sec. 66 r/w.43 IT Act, 384 IPC.	Hacking		66 r/w. 43 IT Act	E-mail Id, FB Profile Hacking and misuse, Server computer hacking by changing password etc.
		Business email ID compromise Fraud		66 r/w. 43 IT Act	Compromising business e-mail IDs, interception of data, sending deceptive e-mail for committing Fraud etc.
		Ransomware		66 r/w. 43 IT Act and 384 IPC	Taking control of a computer system or server by sending malware and demanding money to release.
9	Online IPR Offences Sec.66 (B), 65 IT Act.	Copy Rights violation over		66-B, 65 IT Act and Copy Right Act	Movie uploads, copyright contents uploads.
10	Communal content over Social Media Sec. 153 (A), 505 IPC.	53-A (Depending on the nature of offence), 505 IPC relevant Sub Sections		Morphing images of gods and goddesses and items of religious, importance, and circulation over social media and/or making communal sensitive statements over social media.	Communal content over social media

HOW TO REPORT A CYBER CRIME?

REPORT THE CRIME TO ASSAM POLICE

Reporting at the nearest Police Station: Approach the nearest Police station with a written complaint with a detailed description of the crime. The Officer in Charge of the police station would register an FIR based on the complaint and provide a copy of the FIR with the FIR Number for your future reference.

Reporting online through the National Cyber Crime Portal **https://cybercrime.gov.in**. This is a dedicated online platform for reporting cyber-crimes from anywhere across the country. Though it caters to all types of cyber-crimes, it puts special emphasis on cyber-crimes against women and children. Once a complaint is filed on this portal, it is forwarded to the Police station nearest to the complainant.

Helpline to assist filing of a cyber-crime complaint 155260 (09:00 AM to 06:00 PM)

IMPORTANT POINTS TO REMEMBER

- You can also file a complaint on the Online Cyber Crime Portal Anonymously without giving your identity, the entire complaining process remains same, just that you don't disclose who you are.
- Complainant is advised to block all communications from the fraudster and keep record of all communications as a backup and don't delete any communication neither from the smartphone or the platform where the issue occurred.

STEP BY STEP PROCEDURE TO FILE A COMPLAINT

REPORT CRIME RELATED TO WOMEN OR CHILDREN

https://cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportCPRGRcomplaints-v10.pdf

REPORT OTHER CYBER CRIMES

https://cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportOtherCyberCrime-v10.pdf

IMPORTANT EVIDENCES AND DOCUMENTS TO BE KEPT READY FOR A CYBERCRIME COMPLAINT: -

Social Engineering Frauds: - OTP, KYC, eCommerce, Lottery, Marriage, Job, Data Entry, Dating, Romance and Fake Customer Support Frauds

- Explanation of the issue or offence
- Detailed Bank Statement of the Victim
- Screen Shot of SMS / Links / Email with Complete Header Details
- Copy of the Call Details / Call Recordings

SOCIAL MEDIA FRAUDS: - CYBER BULLYING, CYBER STALKING AND IMPERSONATION

Social Engineering Frauds: - OTP, KYC, eCommerce, Lottery, Marriage, Job, Data Entry, Dating, Romance and Fake Customer Support Frauds

- Explanation of the issue or offence
- Screenshot of Contents/ Profile
- Screenshot of Page URL and Page ID
- Screenshots of the postings done on other websites
  Screenshots of Messages / Call Details/ Call Recordings/ Email with Complete Header Details, where threatening or blackmailing happened
- Contents to be kept ready in both soft and hard copies
- Copy of your ID proof and address proof of the complainant

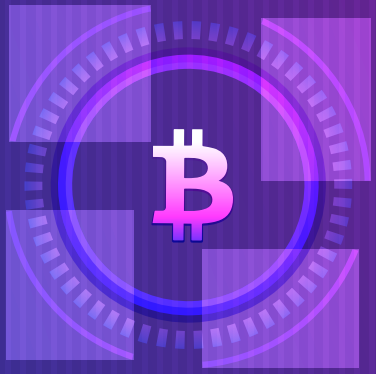
DATA THEFT: -

- Explanation of the issue or offence
- Copy of Data / Copyright Certificate Etc which has stolen
- Suspects Information, If an Employee provide all HR Records including Customer Contacts
- Screenshots of Proof of selling off your copyright data
- Devices used by the suspect
- Contents to be kept ready in both soft and hard copies
- Copy of your ID proof and address proof of the complainant

RANSOMWARE: -

- Explanation of the issue or offence
- Email ID / Contact Details or any other means of communication through which ransom has been demanded
- Screenshots of the suspected Email with full header details
- Contents to be kept ready in both soft and hard copies
- Copy of your ID proof and address proof of the complainant

BITCOIN: -



- Explanation of the issue or offence
- Address / Amount of Bitcoin Involved
- Address from/to whom purchase/sale of Bitcoins is done.
- Screenshots of the suspected Email with full header details
- Contents to be kept ready in both soft and hard copies
- Copy of your ID proof and address proof of the complainant

GUIDELINES BY THE RESERVE BANK OF INDIA: IF YOU BECOME A VICTIM OF A FINANCIAL FRAUD

1) Notify your bank immediately

2) Take an acknowledgment receipt of the complaint from the bank

3) The bank is bound to resolve the complaint within 90 days. This can be done using online portals, calling on the helpline numbers, reporting to home branch etc. The contacts for some of the banks are as shown:

Sl. No.	Bank	Online Portal	Helpline Number
1	HDFC Bank	Report unauthorized transactions tab in www.hdfcbank.com	1860 267 6161
2	State Bank of India	https://cms.onlinesbi.com	1800 11 2211
3	ICICI Bank	www.icicibank.com- Safe Banking – Report an Unauthorized Transaction	1800 2662
4	Kotak Mahindra Bank	https://kapps.kotak.com/FraudPreLogin	1800 209 0000
5	Axis Bank	Report a Fraud Tab in	1860 419 5555

IMPORTANT POINT TO REMEMBER:

If the transaction has happened because of your negligence, that is, because of your sharing your password, PIN, OTP etc., you will have to bear the loss till you report it to your bank. If the fraudulent transactions continue even after you have informed the bank, your bank will have to reimburse those amounts. If you delay the reporting, your loss will increase and it will be decided based on the RBI guidelines and the policy approved by your bank's board.

GENERAL PRINCIPLES REGARDING THE LIABILITY OF THE VICTIM CUSTOMER:

- Zero liability if the fraud is due to the deficiency on the part of the bank
- Zero liability if the fraud was done by a third party and the customer had notified the bank within 3 working days of the fraudulent transaction
- In both cases of zero liability or limited liability of the customer, the banks shall credit the amount due to the victim customer within 10 working days from the date of being notified by the customer
- If the bank is unable to resolve the complaint within 90 days, the bank will anyways have to pay the victim the amount due to him as per the liability rules as mentioned above

INITIATIVES TAKEN BY CID, ASSAM IN CURBING CYBER FRAUDS AND CYBER CRIMES

Citizen Financial Cyber Crime Reporting and Management System

CID Assam has opened a toll free no. 155260 as per the initiatives taken by MHA, Govt. Of India under Indian Cyber Crime Co-ordination Centre(I4C) where any victim can give information about financial frauds within 24 hrs. of commission of such a crime where cyber criminal illegally siphoned off money from their bank a/c, wallet or any other payment gateway . The helpline is operational 24x7 basis and the aggrieved person is required to give a call to this helpline no. with the transaction ID of the fraudulent transaction. The illegally siphoned off money would be blocked if it is still in the process of transfer gateway and returned to the victim after completion of formalities.

You are required to follow the following simple steps-
1. Keep your transaction ID ready for the fraudulent transaction before making a call to the toll-free helpline no.
2. Once you have the transaction ID, call the toll-free helpline no 155260 and provide details to our personnel.
3. Listen to the instructions carefully from our dedicated personnel who will guide you about the steps that you need to take in this regard
4. You are required to lodge one complaint in the portal www.cybercrime.gov.in

The sooner you call and inform the toll-free no., the better is the chance of recovery.
With this, Assam becomes the 8th State in the country to operationalize this toll-free helpline no. for any kind of financial fraud which is a concerted effort on the part of Govt. to make a safe and secure cyber space.
With the operationalization of this toll-free no.w.e.f 28.06.2021 and up to 31.10.2021, Assam Police has been able to block an amount of Rs.1,39,07,899/- (One Cr. thirty nine lacs seven thousand eight hundred and ninety nine only) which was debited from the various accounts of citizens without their knowledge fraudulently.

How to Make an Online Complaint

1. Complaint to RBI
   Please visit the link at https://cms.rbi.org.in/
2. Complaint to SEBI
   Please visit the link at https://scores.gov.in/
3. Complaint to Insurance Regulatory and Development Authority of India (IRDAI)
   Please visit the link at https://igms.irda.gov.in/
4. Complaint to National Housing Bank (NHB)
   Please visit the link at https://grids.nhbonline.org.in/
5. Complaint to Cyber Police Station
   Please visit https://cybercrime.gov.in/

INDIAN CYBER CRIME CO-ORDINATION CENTRE(I4C)

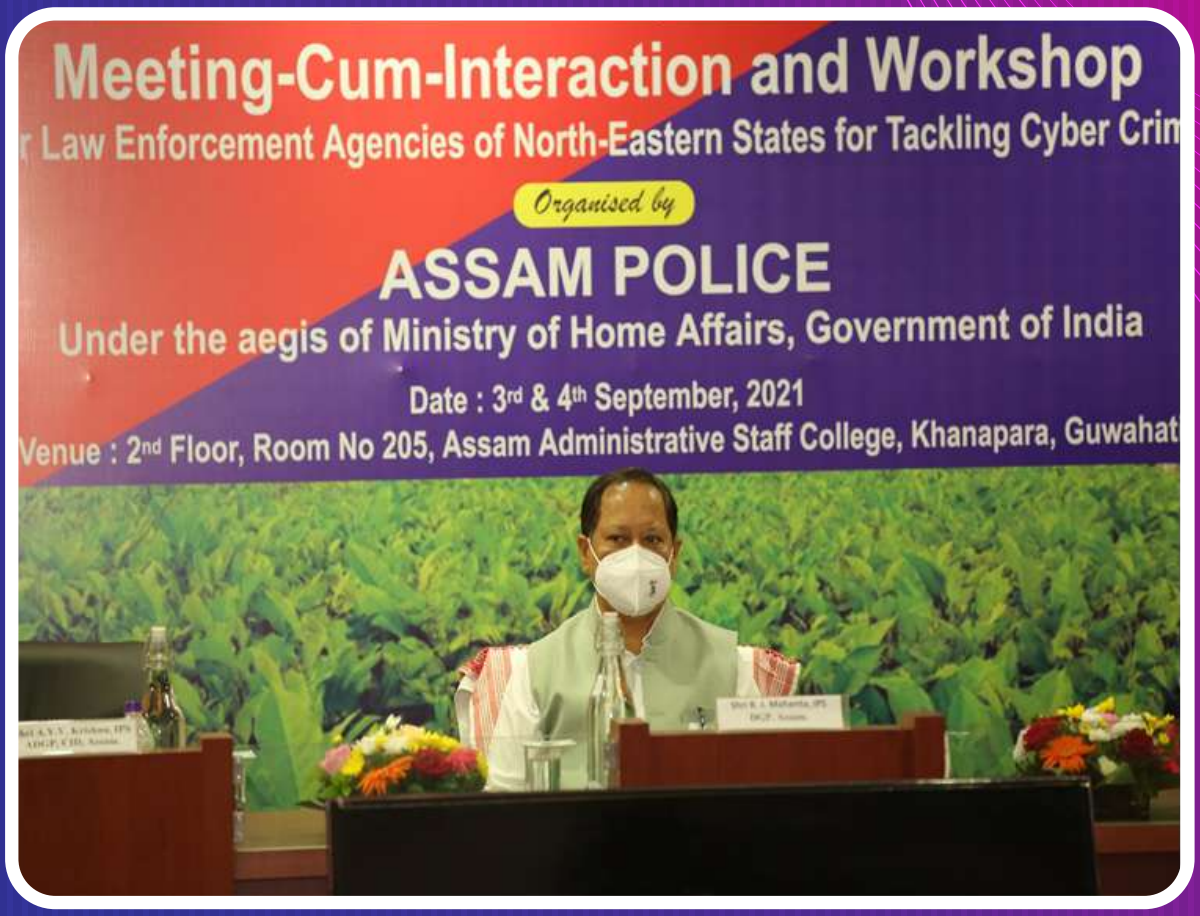
Indian Cyber Crime Co-ordination Centre commonly known as I4C is an initiative by the Ministry of Home Affairs, Govt. of India to effectively deal with the growing incidences of Cyber Crime in the country. The primary idea behind this is that I4C would act as a nodal point in the fight against Cyber Crime. The basic objectives are-

1. To take up R & D activities as per the requirement of Law Enforcing Agencies (LEAs) to develop technologies and tools in collaboration with academic institutions /organisations /universities etc. within the country and in abroad.
2. To prevent the misuse of Cyber space for furthering the cause of anti-social elements, extremist groups , underground outfits waging war against the state.
3. To study cyber laws and suggest / recommend amendments to keep pace with the emerging technologies and ensure international co-operation in combating cyber crime(s).
4. To co-ordinate all activities related to implementation of Mutual Legal Assistance Treaties (MLAT) with other countries related to cyber crimes in consultation with the concerned nodal authority in the Ministry.

KEY COMPONENTS OF I4C

In line with I4C, Regional Cyber Crime Co-ordination Centre (R4C)has been conceptualized to effectively co-ordinate with the states zone wise in dealing Cyber Crimes.
CID, Assam has organized one zonal conference on 2nd and 3rd September, 2021 where representatives from CIS Division, MHA, Govt. of India along with eight north eastern states including Sikkim had participated. In the conference cum in-house discussion, experts in the fields of cyber security and safety had participated and shared their experiences in dealing with various kinds of cyber crime.

SNAPSHOTS OF THE ZONAL CONFERENCE AT ASSAM ADMINISTRATIVE STAFF COLLEGE


Meeting-Cum-Interaction and Workshop
r Law Enforcement Agencies of North-Eastern States for Tackling Cyber Crin
Organised by
ASSAM POLICE
Under the aegis of Ministry of Home Affairs, Government of India
Date : 3rd & 4th September, 2021
Venue : 2nd Floor, Room No 205, Assam Administrative Staff College, Khanapara, Guwahat

DIGITAL INVESTIGATION TRAINING & ANALYSIS CENTRE (DITAC) AND PILOT LAB, SPECIAL BRANCH, HQ, KAHILIPARA, GUWHATI






FEW SNAPSHOTS OF THE 'CYBER CRIME FIRST RESPONDER KIT' TRAINING HELD AT CID HQ--

AWARENESS PROGRAMME ON 'CYBER SECURITY AND CYBER SAFETY'AS A PART OF CYBER JAGROOKTA, AN INITIATIVE OF GOVT. OF INDIA AT B. BAROOAH COLLEGE, GUWAHATI

As a part of initiative of the Govt. towards creating awareness regarding Cyber Crimes among public, an interaction cum in house discussion has been organized by CID, Assam in association with Women Forum of B. Barooah College at the College auditorium.

This is organized as a part of theme Cyber Jagrookta of the Govt. Of India.

TRAINING PROGRAMME AT NORTH EASTERN POLICE ACADEMY(NEPA) ON SEARCH AND SEIZURE OF DIGITAL EVIDENCE

CID, Assam has provided training to Dy.SPs (Proby) from the state of Nagaland & and SI(P)s from Assam Police at North East Police Academy (NEPA), Meghalaya on 'Search and Seizure of Digital Evidence'.

Snapshots of the training in NEPA, Meghalaya

CYBER CRIME PREVENTION AGAINST WOMEN AND CHILDREN (CCPWC) LAB

CID, Assam has one state of art CCPWC lab which is specially designed to deal with Cyber Crimes related to Women and Children. The lab has latest and modern software, hardware and tools which are used to solve Cyber Crimes related to Women and Children and presently catering the demand of all districts of the state who require technical help in this regard. The state of the art lab was inaugurated by hon'ble DGP, Assam in the month of June, 2021 and our dedicated personnel with technical expertise in the field of Cyber Crime are providing necessary assistance to the I/Os on requirement basis.

The specific tools and associated softwares of this lab are -

1. Image/ Video Processing and Mobile Forensics Software
2. GPS Forensics Software & Disk Forensics Software and hardware
3. Online Social Media Monitoring (OSM) Software
4. Data Recovery Hardware and Software
5. Malware Analyser
6. Steganography Tool & CDAMS etc.

Images of the lab

COMPUTER CELL:

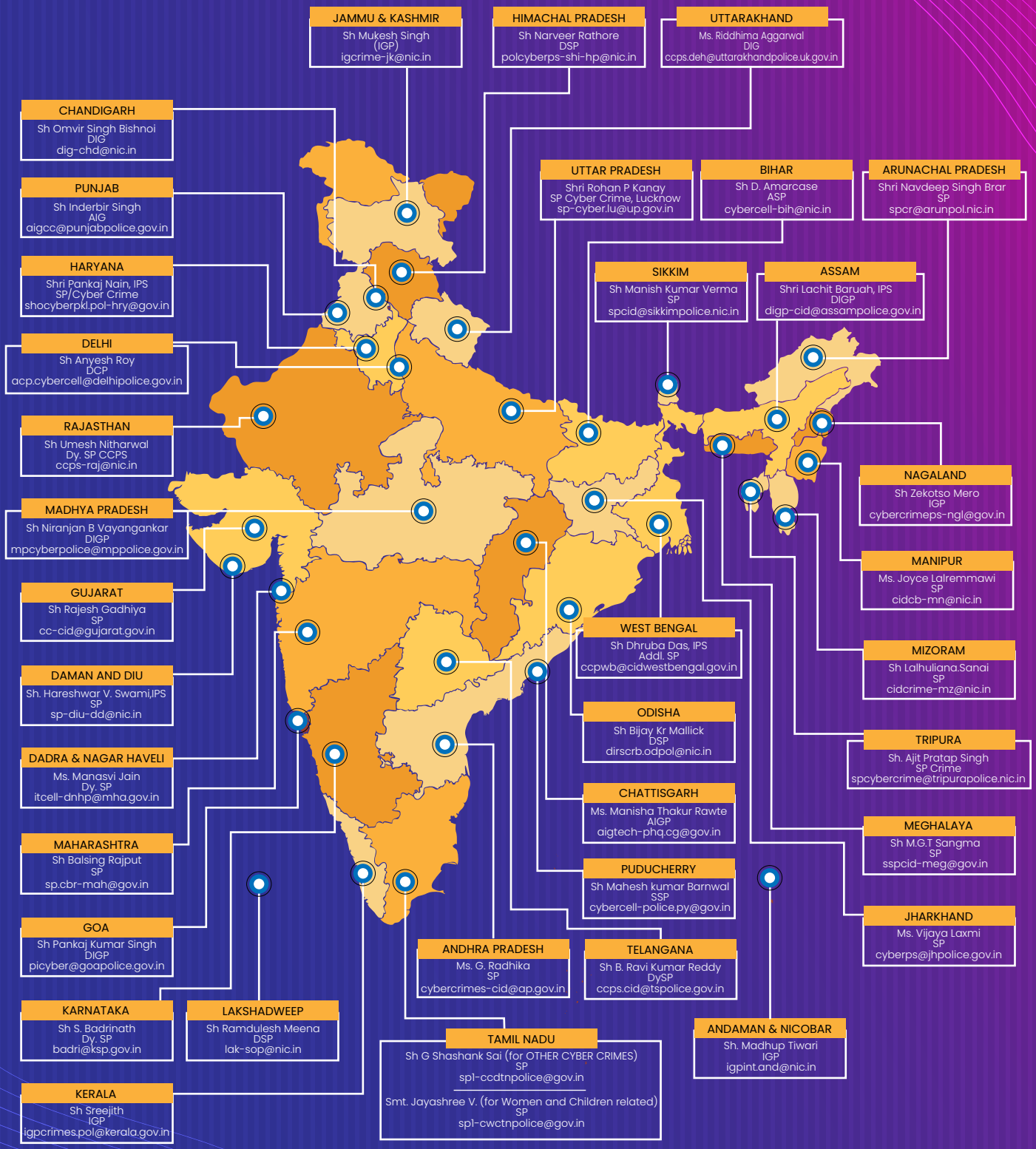
CID, Assam is maintaining a state of the art computer lab with dedicated personnel having expertise in this field equipped with latest technological tools and softwares to deal with the growing instances of Cyber Crime. Our dedicated personnel are providing all kinds of technical help to the respective I/Os investigating cases related to abuse of Cyber Space throughout the entire state. Social media posts and comments are closely monitored to bring to notice any objectionable content/post as per law. Alerts received from I4C (Indian Cyber Crime Co-ordination Centre) which is managed and maintained by CIS division, MHA, Govt. of India regarding latest fraudulent practices and malwares are being sent to all districts by this cell for the benefit of all and to create a safe cyber space.

ASSAM POLICE ACTION ON OBJECTIONABLE SOCIAL MEDIA POSTS

1	NUMBER OF OFFENSIVE POSTS DETECTED AND SENT TO RESPECTIVE DISTRICTS	5097
2	TOTAL NUMBER OF CASES REGISTERED	275
3	TOTAL NUMBER OF PERSONS COUNSELLED	1319
4	NO. OF PERSONS ARRESTED/APPREHENDED	179
6	POSTS DELETED BY USERS	1156
7	POSTS PULLED DOWN THROUGH SERVICE PROVIDER	215
8	TOTAL PULLED DOWN	1371

NODAL CYBER CELL OFFICERS

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

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

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

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

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

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

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

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

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

TAMIL NADU
Sh G Shashank Sai (for OTHER CYBER CRIMES)
SP
sp1-ccdtnpolice@gov.in

Smt. Jayashree V. (for Women and Children related)
SP
sp1-cwctnpolice@gov.in

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

CYBER SECURE

CYBER SECURE

A ONE STOP GUIDE TO STAY SAFE ONLINE

An initiative of

SPECIAL BRANCH

In collaboration with

CRIME INVESTIGATION DEPARTMENT

ASSAM POLICE

https://police.assam.gov.in

/police.assam **/assampolice**

Supported by

END NOW FOUNDATION

ADVOCACY ON DIGITAL SAFETY

www.endnowfoundation.org