

Disclaimer:

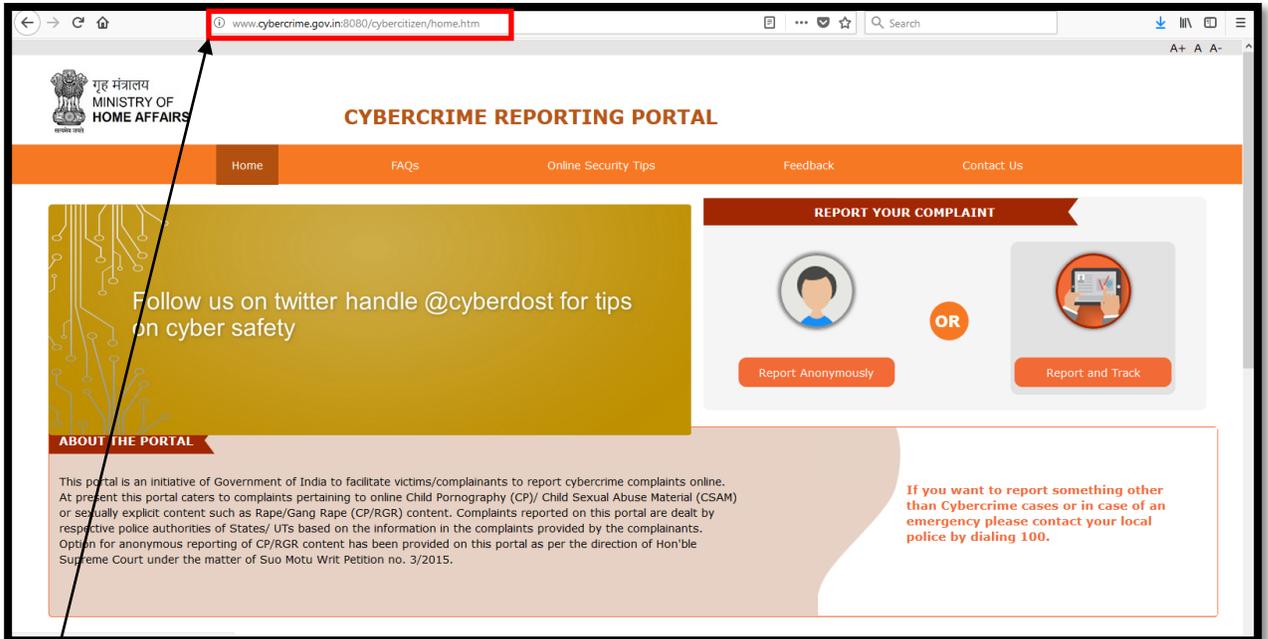
As per Article 246 of the Constitution of India, Public and Police order is the responsibility of the State. Due to transnational and borderless nature of cybercrimes, this Portal has been developed for facilitating public to report cybercrime complaints online.

All the reported complaints are dealt by respective State/UT police authorities based on the information provided by the complainant for necessary action. This portal has been designed to report complaints related to cybercrimes and should not be treated as an FIR. State /UT authorities are responsible for appropriate action on the complaints reported on the portal. Complainants are advised to take care of the accuracy of information provided by them on the portal.

How to Report and Track Complaints

Step 1:

Type the URL <https://www.cybercrime.gov.in> in the Web Browser



Step 1

USER MANUAL FOR CYBERCRIME REPORTING PORTAL

Step 2:

Select “**Report and Track**” option, if you want to report an online Child Pornography (CP) - Child Sexual Abuse Material (CSAM) or sexually explicit content such as Rape/Gang Rape (CP/RGR) content by revealing your identity like name, mobile number, e-mail id, etc..



Step 2

USER MANUAL FOR CYBERCRIME REPORTING PORTAL

Step 3:

- Enter your First name.
- Enter your valid Indian mobile number and click on “**send OTP**”. You will receive an OTP in the registered mobile number (OTP will be valid for 30 minutes). Enter the same OTP in the “**OTP**” field.
- Enter the Captcha, then press “**Submit**”.

The screenshot displays the 'CYBERCRIME REPORTING PORTAL' login interface. The page header includes the Ministry of Home Affairs logo and the text 'गृह मंत्रालय MINISTRY OF HOME AFFAIRS'. The main content area is titled 'Cyber Crime > Login' and features a 'Login' button. Below this, there are two tabs: 'Citizen Login' (selected) and 'Authorized Agency Login'. The 'Citizen Login' form contains fields for 'First Name', 'Mobile No.', and 'OTP'. A 'Send OTP' button is positioned to the right of the 'Mobile No.' field. Below the 'OTP' field, there is a captcha image showing the characters '3e7z' and a 'Submit' button. A 'Clear' button is located below the 'Submit' button. A blue callout box on the right side of the form displays the message: 'Your OTP is 9975 for login to Cyber Police Application. This OTP will expire after 30 minutes.' Three red boxes with arrows point to the 'First Name' field, the 'Send OTP' button, and the 'Submit' button, labeled 'Step 3', 'Enter the OTP', and 'Enter Captcha' respectively. The footer of the page contains the text 'Website Content Managed by Ministry of Home Affairs, GoI' and 'FeedBack | Contact Us |'.

Step 4:

Provide the details as required for reporting a complaint.

a. Enter the Crime incident details

- i. Select "Category of Crime" from the drop-down list (**Mandatory**) - Three options available in drop-down –
 1. Rape/ Gang rape (RGR) – sexually abusive content
 2. Obscene content
 3. Child Pornography (CP) - Child Sexual Abuse Material (CSAM)
- ii. Select "Date of Incident"
- iii. Enter "Time of incident"
- iv. Enter details of "Social Media Type on which the incident happened" – Mention the name of social media platform where you have received CP/RGR content.
- v. Enter the "Social Media Username/ ID/ URL" – Mention the username/ ID/ URL of social media platform (like Facebook, WhatsApp, Twitter, YouTube etc.) where CP/RGR content is present. In case of WhatsApp, please mention the mobile number from which you have received the CP/RGR content.
- vi. Enter the "e-mail address" – In case, you have received any CP/RGR content through e-mail attachment.
- vii. Enter "Website/ URL where the content was found" – Mention the URL or the website name, where the CP/RGR content is present.
- viii. Type Incident description in the box

b. Enter the Suspect details

- i. Enter the suspect name (If known)
- ii. Enter the corresponding address of suspect like state, district, colony, street name etc. so that it could help the police authorities in investigation.

c. Enter the Complainant details

- i. Enter your Name (**Mandatory**) – As mentioned during registration.
- ii. Mobile Number will be filled automatically (as mentioned during registration)
- iii. Enter your e-mail ID
- iv. Enter your relationship with the victim
- v. Select Country, State (**Mandatory**) and District
- vi. Select Police station and type Pin Code

d. Upload the Evidence

- i. Enter the description about the evidence
- ii. Upload evidence as attachment

e. After the above details are filled in the portal, click on "**submit** button".

Note: All the fields with red asterisk "*" are mandatory to be filled in the portal.

USER MANUAL FOR CYBERCRIME REPORTING PORTAL

The screenshot displays the 'CyberCrime Reporting Portal' interface. At the top, it shows the Ministry of Home Affairs logo and the portal name. The user is logged in as 'User1 xyz' on '31/12/2018' at '17:41'. The page title is 'CyberCrime'. On the left, there are navigation links: 'Report Anonymously', 'Update Mobile Number', 'Report Cyber Crime', 'Check Status', and 'FAQ'. The main form is divided into several sections:

- Crime/Incident Details:** Includes 'Category of Crime' (dropdown menu), 'Approximate date & time of incident/receiving/viewing of content' (text input), 'Information Source' (dropdown menu), and 'Other Social Media' (text input with an 'Add' button). A text area for 'Please provide any additional information about the incident' is also present.
- Suspect Details:** Includes 'Suspect Name' (text input), 'Corresponding Address' (checkbox for 'Do you want to share correspondence address?'), and a form for address details (House No., Street Name, Colony, Village / Town / City, Tehsil, Country, State, District, Police Station, Pincode).
- Complainant Details:** Includes 'Name', 'Mobile No.', 'Relationship with the victim', 'Email', and another 'Corresponding Address' form.

A red box labeled 'Step 4' is positioned on the left side of the form. Four arrows originate from this box and point to the following elements in the form:

- The 'Category of Crime' dropdown menu.
- The 'Information Source' dropdown menu.
- The text area for 'Please provide any additional information about the incident'.
- The 'State' dropdown menu in the 'Corresponding Address' section of the 'Complainant Details'.

Step 5:

On submission of the complaint, a complaint submission message will be displayed on the portal and complaint would be worked upon by the respective State/UT police authorities.

- Once you click on the “**click here to print**” option, details of the complaint reported gets downloaded in PDF format, which could be used for further reference.
- You will also receive a message and e-mail on the registered mobile number and e-mail ID once the complaint is successfully submitted in the portal.

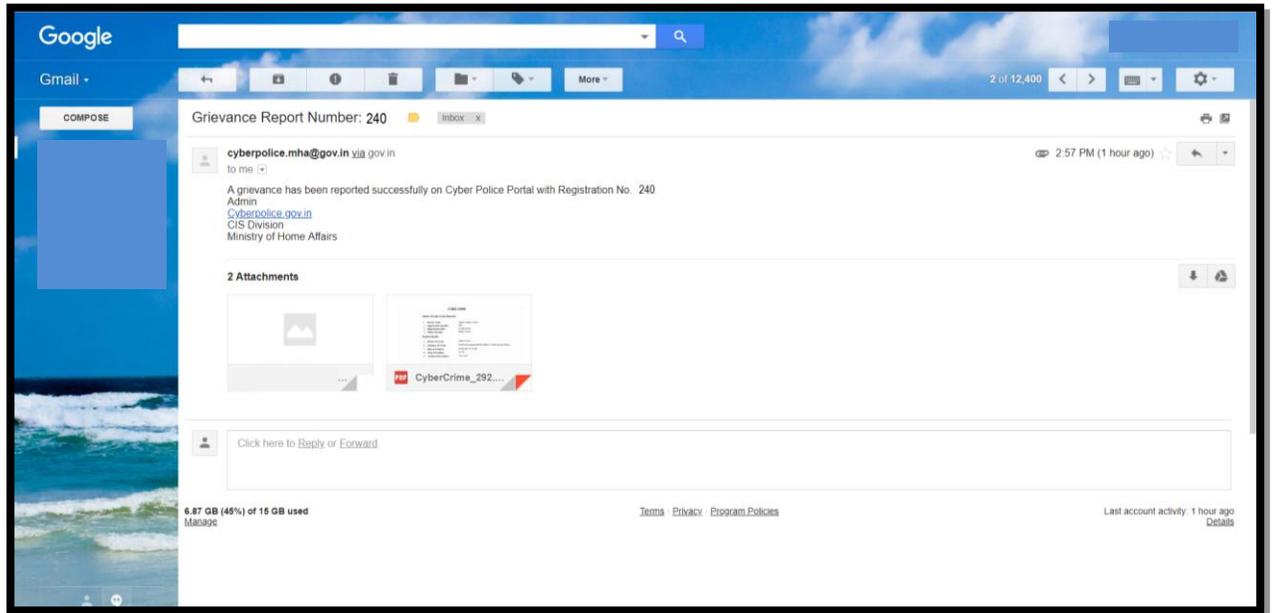
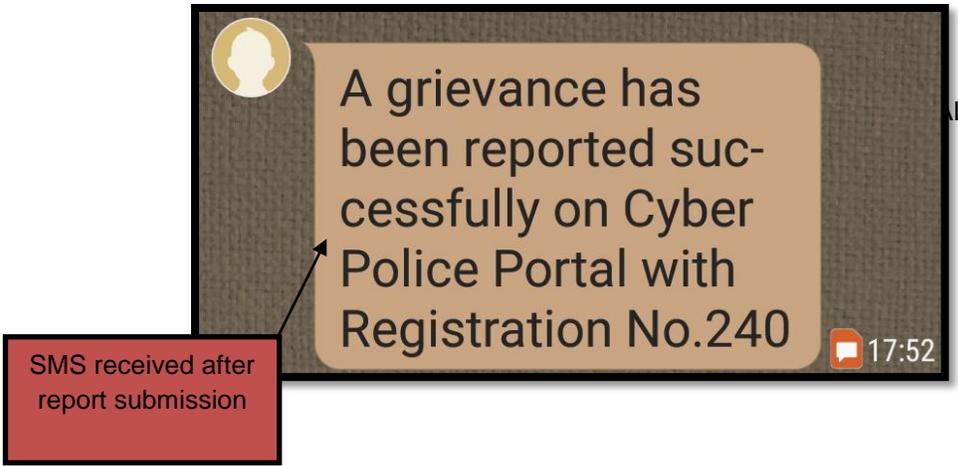
USER MANUAL FOR CYBERCRIME REPORTING PORTAL

The screenshot shows the CyberCrime Reporting Portal interface. At the top left is the logo of the Ministry of Home Affairs. The header includes the text 'CYBERCRIME REPORTING PORTAL' and user information: 'User: John', 'Date: 28/06/2018', and 'Time: 16:41'. A navigation bar contains 'Cyber Crime > Login > CyberCrime' and 'CyberCrime' with a notification bell icon. A green message box at the top states: 'The complaint has been successfully submitted. Click here to print.' Below this is the 'Crime/Incident Details' form. A red box highlights the success message, and an arrow points from a 'Step 5' box to it. The form fields include: 'Category of Crime*' (dropdown), 'Date of Incident*' (calendar), 'Time of Incident' (10:00, 24 hours format), 'Social Media on which incident occurred' (dropdown), 'Social Media Username/ID/url', 'E-Mail' (someone@example.com), and 'Website/URL where the content was found' (www.example.com). There is an 'Add' button and a table with columns 'S.No.', 'Website/URL where the content was found', and 'Delete'. An 'Incident Description*' field is also present.

The screenshot shows the 'CYBER CRIME' report details page. It lists the following information:

- CYBER CRIME**
- Details of Cyber Crime Reported**
- 1. Service Type: Report Cyber Crime
- 2. Registration Number: 240 (highlighted with a red box)
- 3. Registration Date: 12/06/2018
- 4. Mobile Number: 9XXXXXXXXX
- Incident Details**
- 5. Nature of Crime: Cyber Crime
- 6. Category of Crime: Child Pornography(CP)/Child Sexual Abuse Material
- 7. Date of Incident: 02/06/2018
- 8. Time of Incident: 10:00:00
- 9. Incident Description: abc123 has shared a CSAM in www.abc.com
- 10. Place of Incident:
- 11. Description of the Evidence: abc123

Registration number for tracking



Step 6:

In case you want to track the status of your complaint, click on “**Check Status**” option and select date to search for your registered complaint.

Also, progress of the reported complaint would be notified to the registered mobile number.

USER MANUAL FOR CYBERCRIME REPORTING PORTAL

The screenshot shows the 'CYBERCRIME REPORTING PORTAL' interface. On the left, a navigation menu includes 'Check Status', which is highlighted with a red box. An arrow points from this box to a red box labeled 'Step 6'. The main content area displays a table of reported cases with columns for Sr.No., Service No., Service Type, Date Filed, Status, and Status Date. Row 19 is highlighted in red, showing 'FIR Registered' status. A search bar at the top allows filtering by date range.

Sr.No.	Service No.	Service Type	Date Filed	Status	Status Date
11	227	Cyber Crime	07/06/2018	Registered	07/06/2018
12	232	Cyber Crime	12/06/2018	Registered	12/06/2018
13	233	Cyber Crime	12/06/2018	Registered	12/06/2018
14	234	Cyber Crime	13/06/2018	Registered	13/06/2018
15	236	Cyber Crime	16/06/2018	Registered	16/06/2018
16	237	Cyber Crime	16/06/2018	Registered	16/06/2018
17	238	Cyber Crime	16/06/2018	Registered	16/06/2018
18	239	Cyber Crime	16/06/2018	Registered	16/06/2018
19	240	Cyber Crime	16/06/2018	FIR Registered	16/06/2018
20	275	Cyber Crime	19/06/2018	Registered	19/06/2018

Step 6

The screenshot shows an SMS conversation titled 'AX-PMASMS'. The messages are as follows:

- Message 1 (17:52): "A grievance has been reported successfully on Cyber Police Portal with Registration No.240"
- Message 2 (18:56): "Dear [redacted], Cyber Crime No :240 is accepted and is under process"
- Message 3 (19:06): "Dear [redacted], For Cyber Crime No :240 FIR is registered"

Two red boxes on the left provide context for the messages:

- "SMS received after the case is accepted" points to the second message.
- "SMS received after FIR is registered" points to the third message.

SMS received after the case is accepted

SMS received after FIR is registered

USER MANUAL FOR CYBERCRIME REPORTING PORTAL

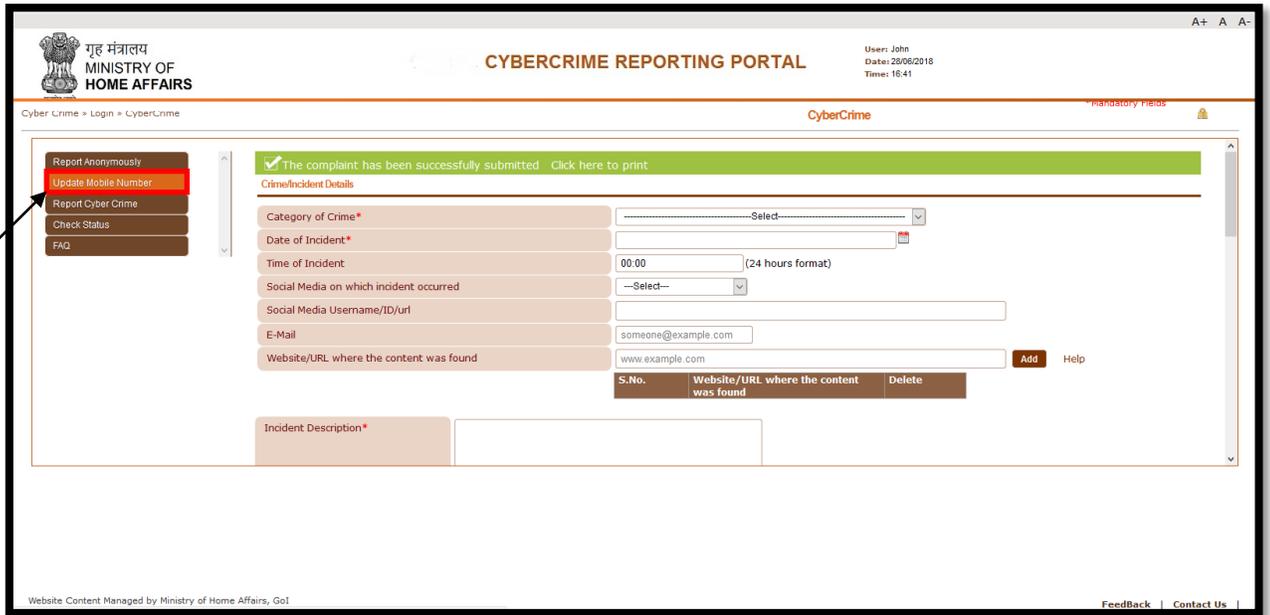
Step 7:

Updating your mobile number.

- I. In case, you want to update your registered mobile number, click on **“Update Mobile Number”** after logging in **“Report and Track”** option.
- II. Enter your new mobile number in **“New Mobile Number”** field and click on **“verify mobile number”**
- III. Enter the OTP received in updated mobile number.

All the cases registered on the old mobile number will be mapped to new mobile number.

Step 7
(i)



Step 7
(ii)

