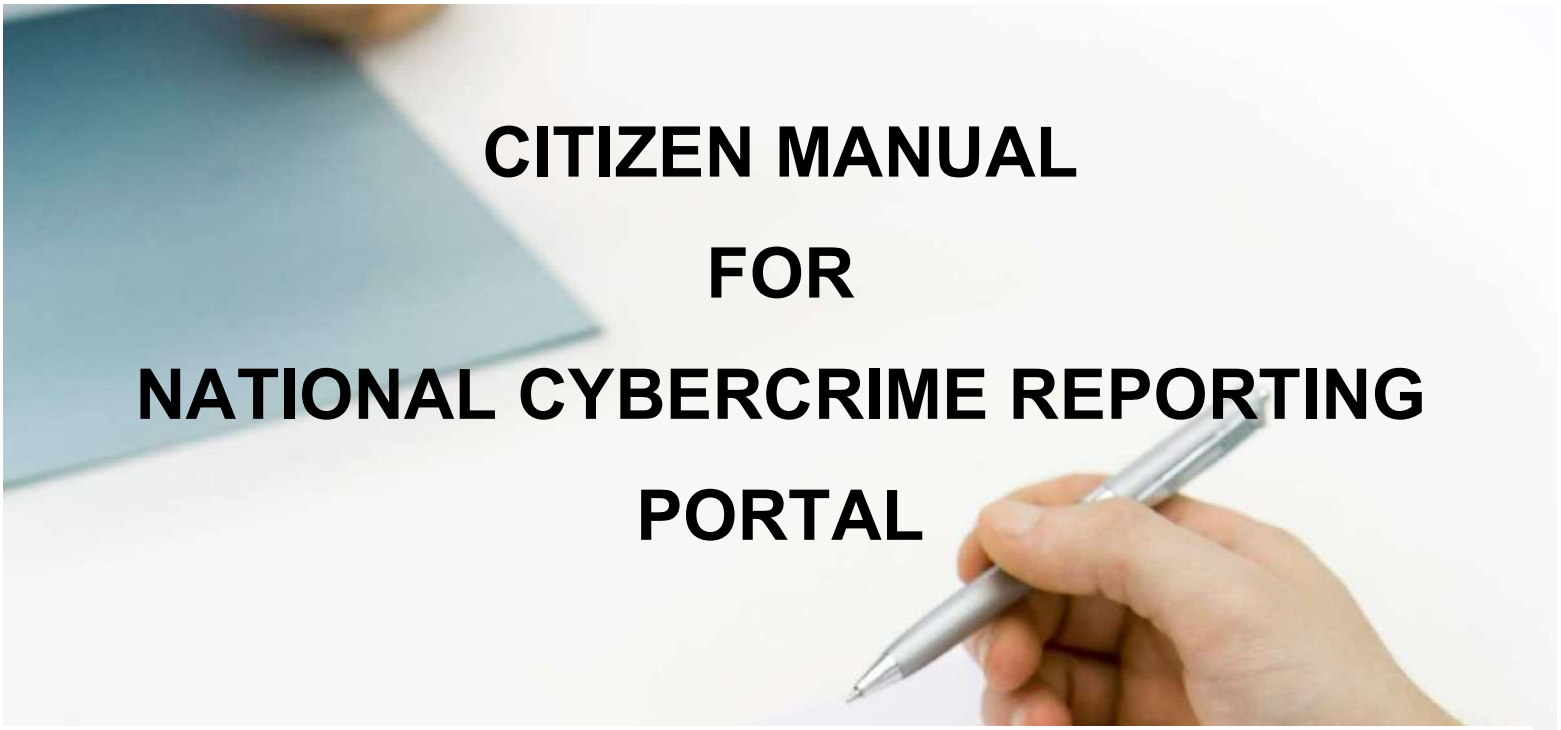


CITIZEN MANUAL

FOR

NATIONAL CYBERCRIME REPORTING PORTAL

INDIAN CYBERCRIME COORDINATION CENTRE (I4C)

MINISTRY OF HOME AFFAIRS

सत्यमेव जयते
Goverment Of India

USER MANUAL FOR REPORTING CYBER CRIMES (except Child Pornography, Rape/Gang Rape and Obscene Content related Cybercrimes)

Ministry of Home Affairs

Document Information

Owner	Ministry of Home Affairs, Government of India
Document Status	Final
Date Effective	30 Aug 2019

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.

ABBREVIATIONS

OTP	One Time Password
2FA	Two factor Authentication
EML	Electronic Mail
BTC	Bitcoin
TAU	National Cybercrime Threat Analytics Unit
NCFL	National Cybercrime Forensic Laboratory
NCTC	National Cybercrime Training Centre
NCR&IC	National Cyber Research and Innovation Centre
JPG/JPEG	Joint Photographic Experts Group
AVI	Audio Video Interleave
MP4	MPEG-4 AVC (Advanced Video Coding)
FLV	Flash Video
MPEG	Moving Picture Experts Group
AMR	Adaptive Multi-Rate
DVI	Digital Video Interactive
PDF	Portable Document Format
PNG	Portable Network Graphics
WMV	Windows Media Video
3GP	3GPP file format
Doc	Document

1. Background

Ministry of Home Affairs, Government of India has set up 'Indian Cyber Crime Coordination Centre (I4C)' to deal with cybercrimes in a coordinated and comprehensive manner. Following are seven components of the centre:

1. National Cybercrime Threat Analytics Unit (TAU)
2. National Cybercrime Forensic Laboratory (NCFL)
3. National Cybercrime Training Centre (NCTC)
4. Cybercrime Ecosystem Management
5. Platform for Joint Cybercrime Investigation Team
6. National Cybercrime Reporting Portal
7. National Cyber Research and Innovation Centre (NCR&IC)

One of the components of I4C is operationalisation of National Cybercrime Reporting Portal to deal with all types of cybercrimes. The earlier Cybercrime Reporting Portal www.cybercrime.gov.in was for filing of cybercrime complaints pertaining to Child Pornography (CP)/ Rape Gang Rape (RGR)/ Obscene Content only, however, the National Cybercrime Reporting Portal facilitates filing of all types of cybercrimes with special focus on the cybercrime against women and children.

2. Introduction

Working of the Portal

i. This portal facilitates a person to report any kind of cybercrime under various available category and sub-category, including cybercrimes affecting women and children. List of the categories and subcategories is provided on **Annexure 'A'**

ii. There is a dedicated section '**Learn about Cybercrime**' on the home page of cybercrime.gov.in portal under which you can find out description of various type of cybercrime that can be reported through this portal

iii. Assignment of a reported complaint to a State/UT is done on the basis of the address of the complainant.

iv. For future tracking of the complaint, the complainant will receive a complaint ID on the registered mobile number and e-mail address. This complaint ID is not an FIR number but is a confirmation of registration of complaint on the portal.

v. The jurisdictional State/UT law enforcement agency will also send the update of action taken on the registered mobile number and e-mail ID.

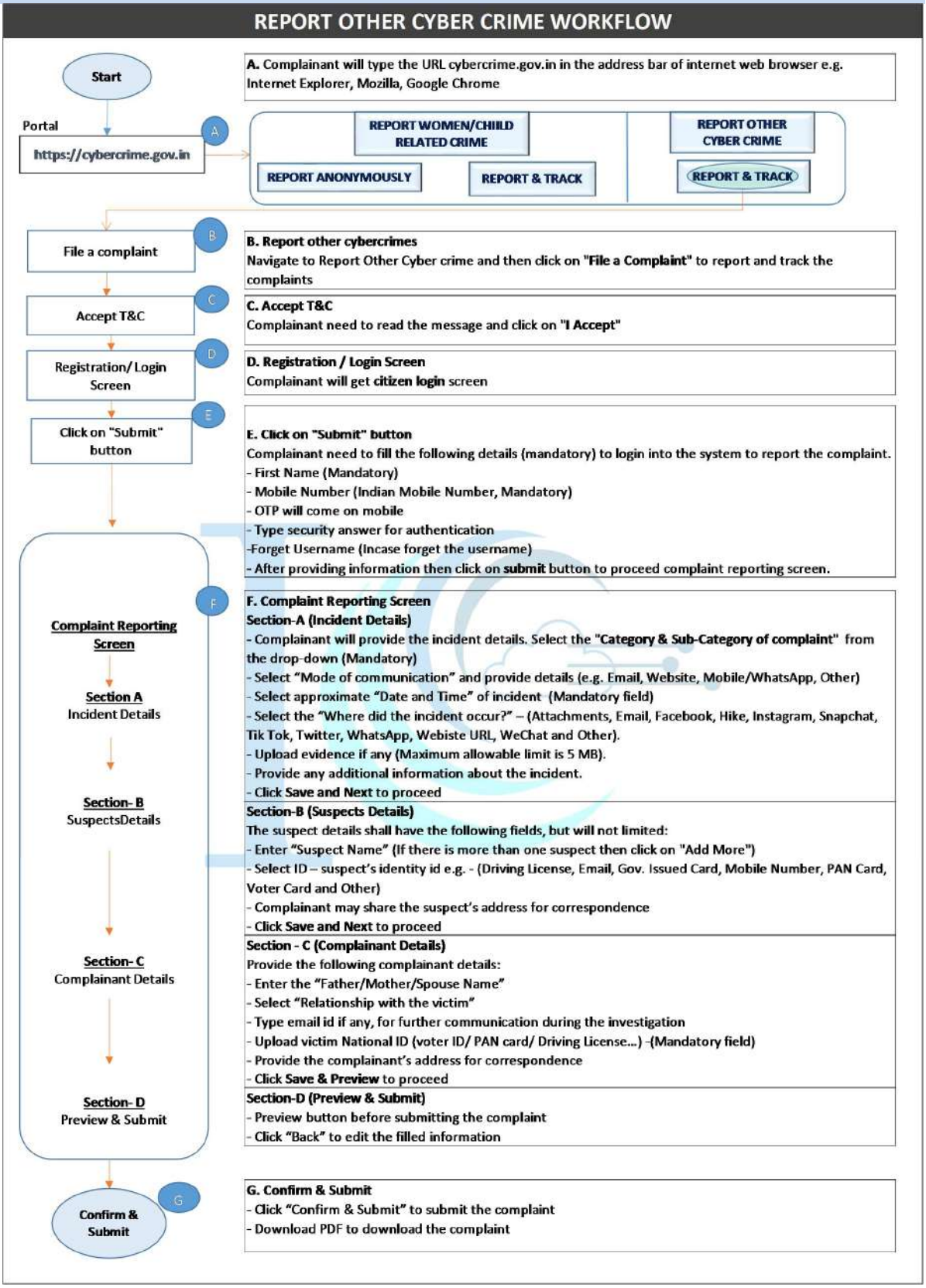
vi. In case complainant is not satisfied with the action taken by the State/UT law enforcement agency he/she can reach out to grievance officers of the concerned State/UT.

vii. The complainant can track status of his/her reported complaint by logging into the account

Purpose

- The purpose of this citizen manual document is to describe the functionalities and workflow that is provided to citizens on the cybercrime portal for reporting other cybercrimes (excluding Child Pornography, Rape/Gang Rape and Obscene Content related Cybercrimes) complaints.
- In addition to the information contained herein, further guidance can be found in the Help and Sample of evidences in **Annexure 'B'** and **Annexure 'C'**

3. Report Other Cybercrime Flowchart



4. HOW TO REPORT A COMPLAINT

Type the URL https://www.cybercrime.gov.in in the Web browser

Step 1: Navigate to Report Other Cyber Crime section

Select **Report Other Cyber Crime**,if you want to report an online cybercrime such as Online and Social Media Related Crime, online financial frauds, hacking, cryptocurrency crime, online job fraud, online matrimonial fraud, and other cyber crimes. Following are the steps to report a cyber crime complaint:

I. Click on "**File a complaint**"

II. Read the message carefully in the window and check on the "**I Accept**" checkbox.

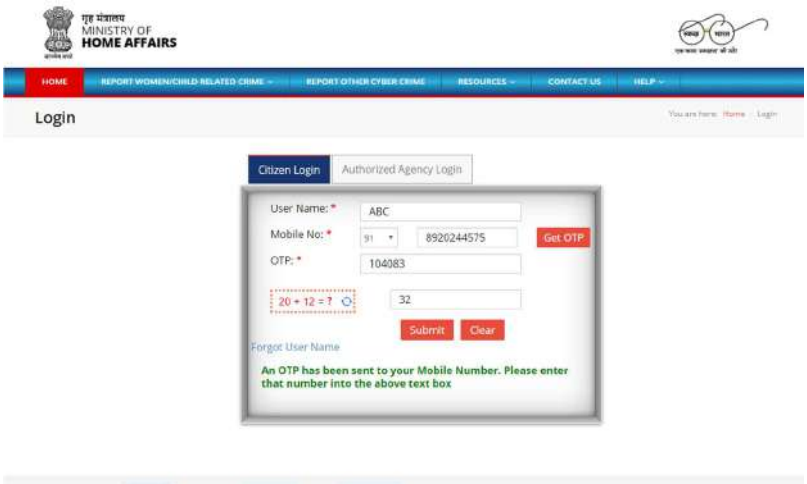
III. Under Report Other Cyber Crime, click on "**Report Other Cyber Crime".** Also accessed from "**HOME**" page :

Step 2: Login for reporting a complaint

You will need to register yourself using your mobile number. You will receive a One Time Password (OTP) that will be used to verify your phone number. The OTP is valid for 30 minutes. Once you successfully register your mobile number on the portal, you will be able to report the compliant.

You required to fill the following details (mandatory) to login into the portal to report your complaint.

i. Enter your name in "**User Name**" field (mandatory)
ii. Enter your **Mobile Number** (mandatory)
iii. Click on **Get OTP**
iv. Enter the OTP (received on mobile number) (mandatory)
v. Enter the security answer for authentication in the field provided
vi. Click on **Submit** button



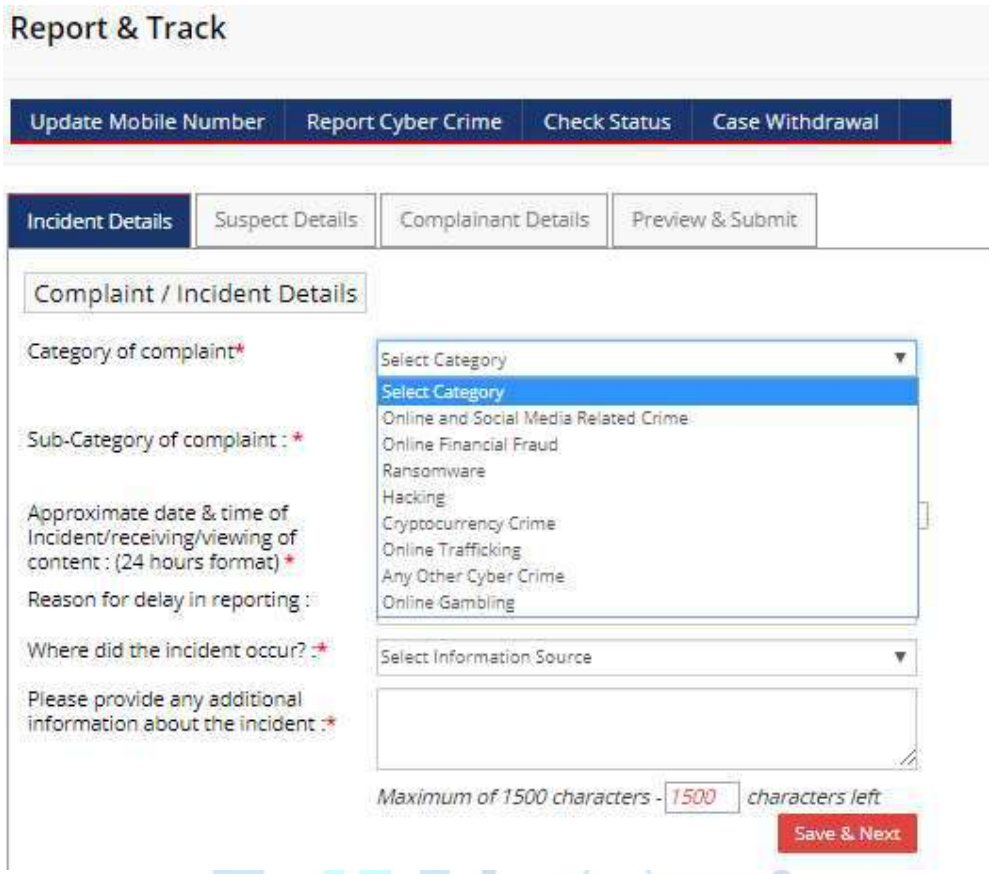
Step 3: Select category and sub-category of Complaint

From this portal, complainants can report online cyber crime complaints. For each category and sub-category detailed steps are mentioned below.

Under **Incident details** tab, select the category of complaints.

a. Select "Category of complaint" (Mandatory) from the drop-down (following Eight options are availabe in drop-down) :

1. **Online and Social Media Related Crime**
2. **Online Financial Fraud**
3. **Ransomware**
4. **Hacking**
5. **Cryptocurrency Related Crime**
6. **Online Trafficking**
7. **Online Gambling**
8. **Any Other Cyber Crime**

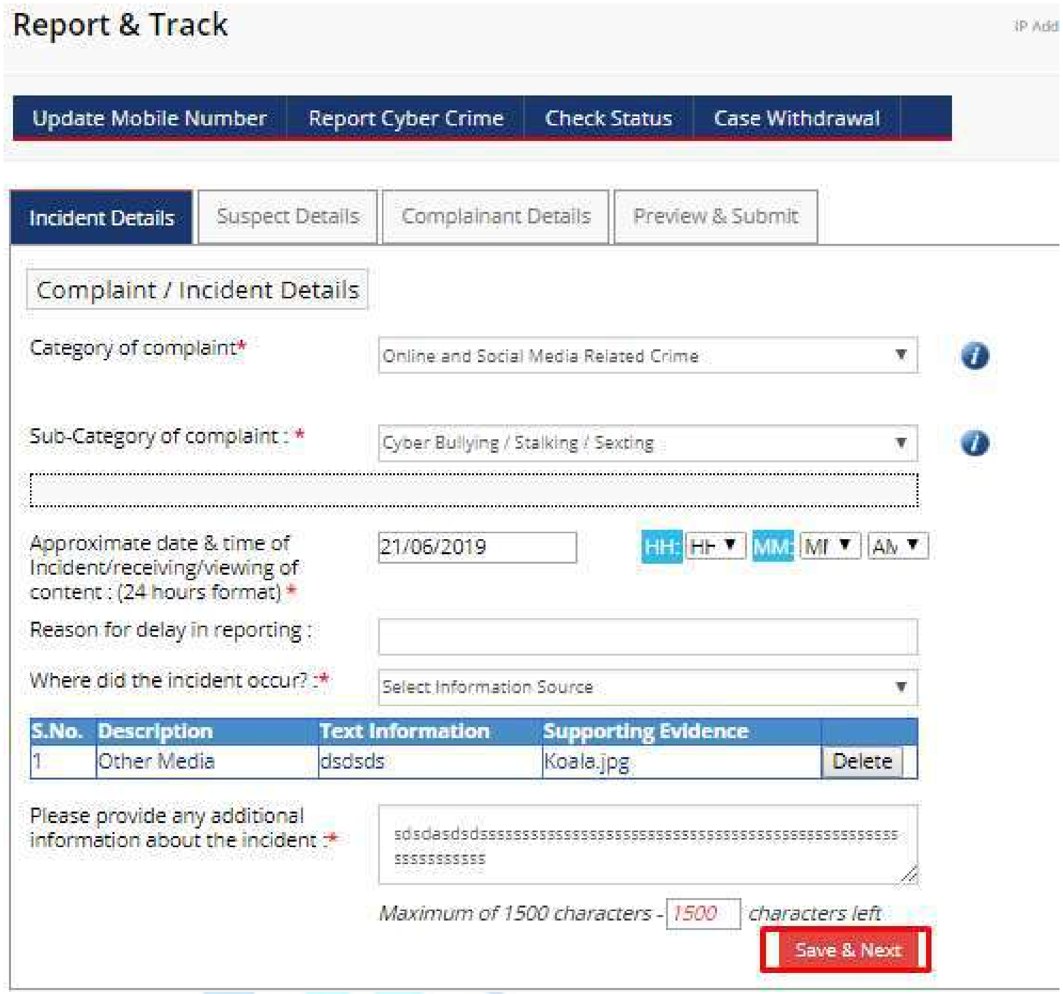


b. Similarly, select the "**Sub-Category of Crime"** (Mandatory) from the drop-down for the respective cybercrime category.

Step 4: Provide Incident Details

Fill the following details about the complaint/incident details

i. Select approximate "Date and Time" of incident (Mandatory)
ii. Give "Reason for delay in reporting"
iii. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, twitter, Instagram etc.), messaging platform (WhatsApp, hike etc.), e-mail, website, URL or other (Mandatory)
iv. Enter email Id (Mandatory) if select other no mail ID required
(Note: For help on uploading evidence refer **AnnexureB** Help,Section 10)
v. Upload evidence if any *(Maximum allowable limit is 5 MB).* (Mandatory)
vi. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)
vii. Click on **Save and Next** to proceed

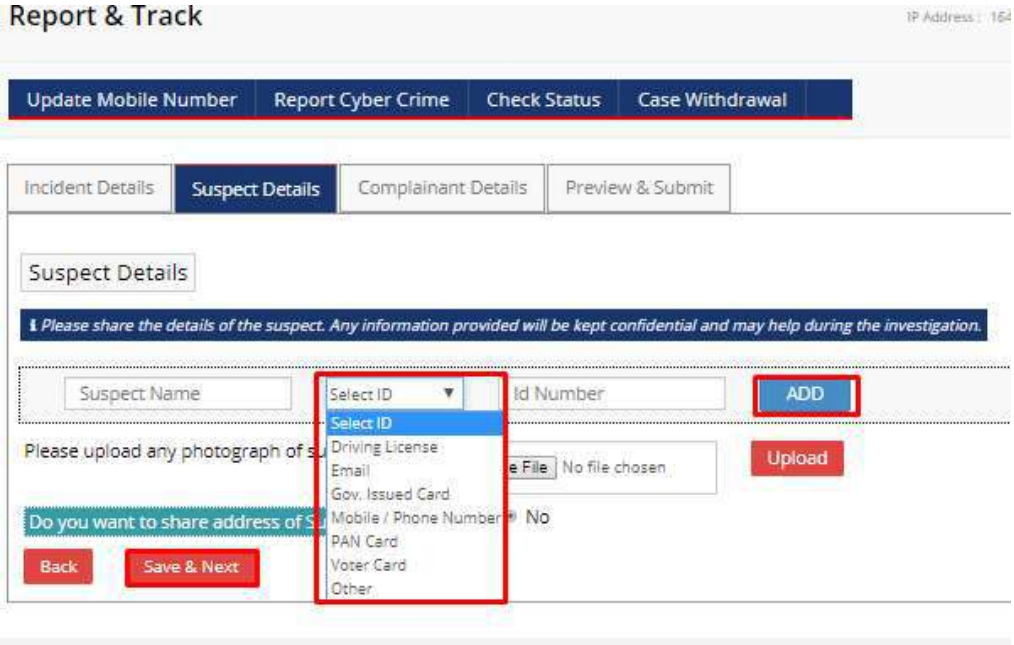


Step 5: Provide Suspect Details

Share the suspect details if suspect is known.

a. Enter "**Suspect Details**" to help in investigation

i. Enter "Suspect Name" (If there is more than one suspect than click on Add More)
ii. Select ID – Provide suspect's identity id e.g. (Driving License, Email, Gov. Issued Card, Mobile Number, PAN Card, Voter Card and Other) then click **Add** and subsequently add the selected details.
iii. Please upload any photograph of suspect.



b. You may share the suspect's address for correspondence if known (Click on **Yes** and fill the below details)

i. Type house no., street name, colony, village/town/city, tehsil details
ii. Select "Country"
iii. Select "State"
iv. Select "District"
v. Select "Police Station"
vi. Enter "Pin code" number
vii. Click **Save & Next**

Step 6: Provide Complainant Details

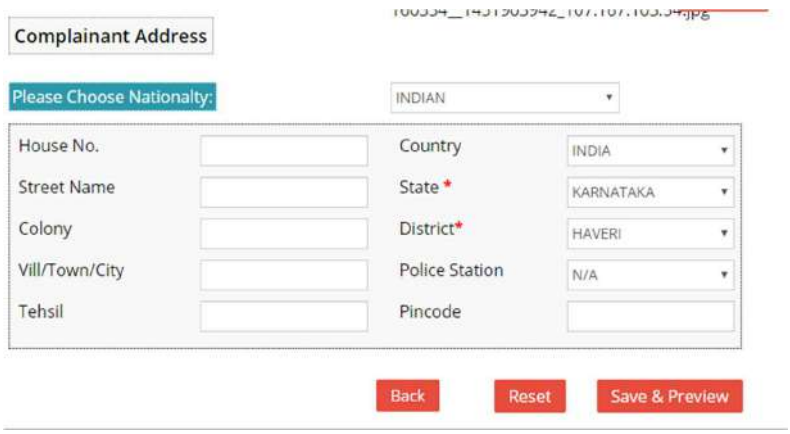
Click on "**Complainant Details**" tab to provide the details of complainants

a. Fill the complainant details

i. Select the “Gender” & Enter “DOB”.
ii. Enter the “Father/Mother/Spouse Name” details (Mandatory)
iii. Select “Relationship with the victim”
iv. Provide your email id if any, for further communication during the investigation
v. “Upload victim National ID (voter ID/ PAN card/ Driving License or any Govt. issued card)” - (Mandatory)

b. Provide the complainant’s address for correspondence

i. Select Your “Nationality”
ii. Type House no., Street Name, Colony, Tehsil details
iii. Type Village/Town/City
iv. Select “Country” (By default India)
v. Select “State” – (Mandatory)
vi. Select “District” - (Mandatory)
vii. Select “Police Station”
viii. Enter “tehsil”
ix. Enter “Pin code” number
x. Click **Save & Preview**



Step 7: Preview & Submit

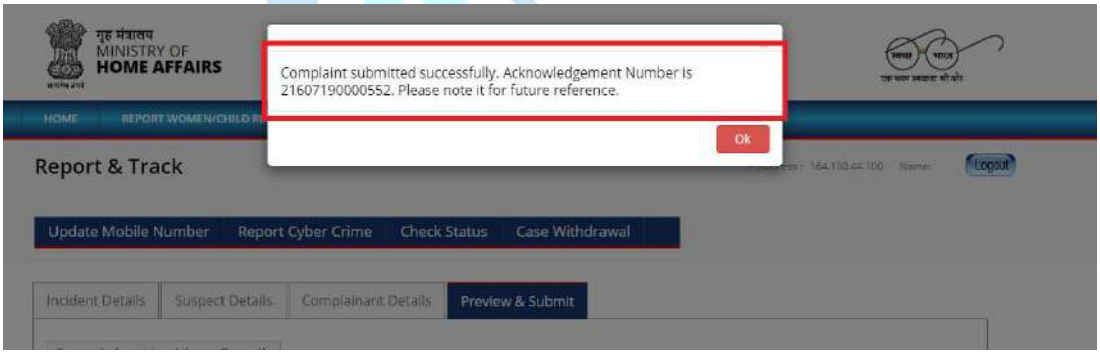
Click on "**Preview & Submit**" tab to review the information you provided before submission of the complaint

a. Click "**Reset**", if you want to edit the filled information, or

b. Check "**I Agree**" Button

c. Click "**Confirm & Submit**" to submit the complaint

On submission of the complaint, a complaint submission confirmation message with 'Complaint ID' will be displayed on the portal

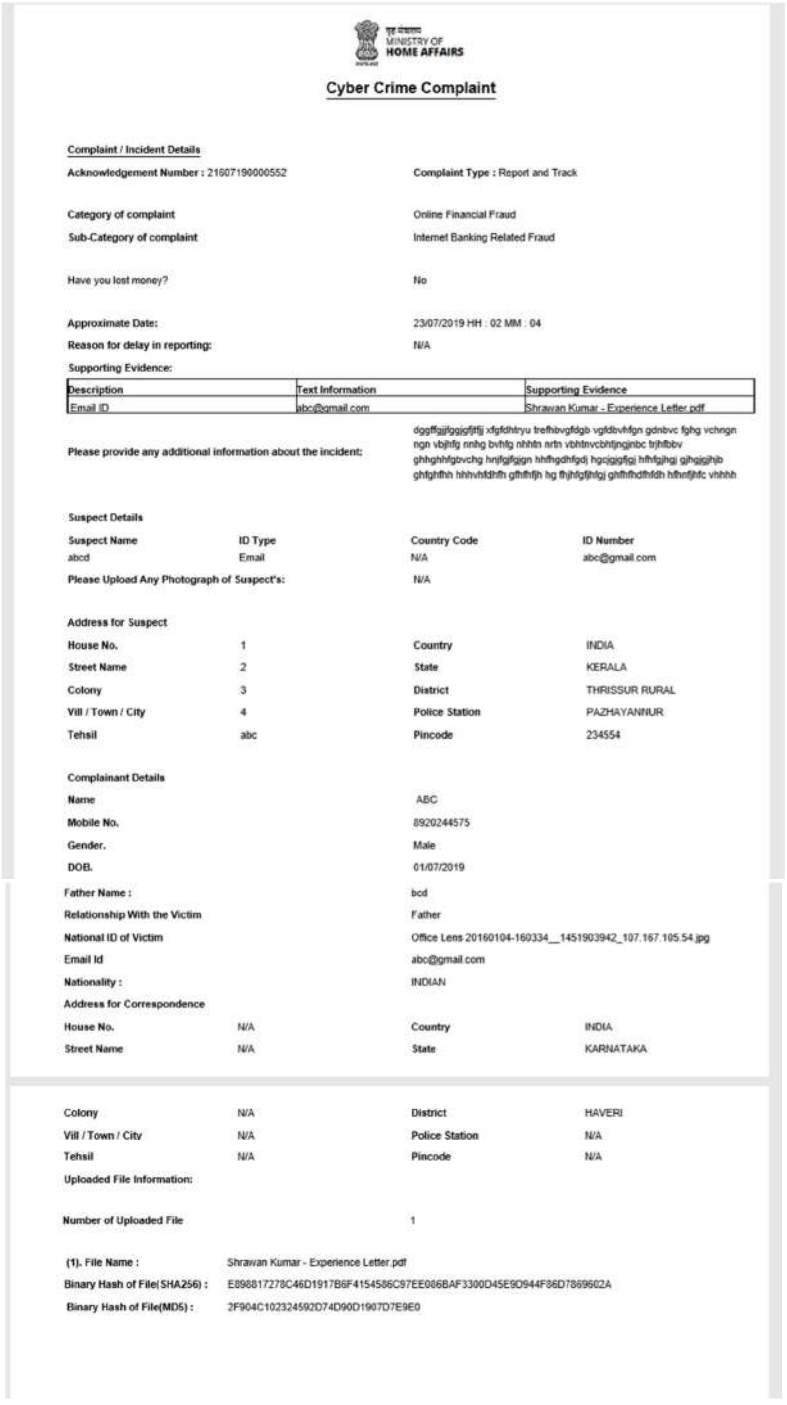


You will also receive a message and e-mail on the registered mobile number and e-mail ID once the complaint is successfully submitted on the portal.

Step 8: Generate PDF of reported complaint

If you want to download the complaint, click on the "**Download PDF**" option, details of the complaint reported gets downloaded in PDF format, which could be used for further reference.

Following are the sample of downloaded complaint



MINISTRY OF HOME AFFAIRS

Cyber Crime Complaint

Complaint / Incident Details

Acknowledgement Number : 21607190000552 — **Complaint Type :** Report and Track

Category of complaint	Online Financial Fraud
Sub-Category of complaint	Internet Banking Related Fraud
Have you lost money?	No
Approximate Date:	23/07/2019 HH : 02 MM : 04
Reason for delay in reporting:	N/A

Supporting Evidence:

Description	Text Information	Supporting Evidence
Email ID	abc@gmail.com	Shrawan Kumar - Experience Letter.pdf

Please provide any additional information about the incident: dggffgjjfggjgfjtfjj xfgfdhtryu trefhbvgfdgb vgfdbvhfgn gdnbvc fghg vchngn ngn vbjhfg nnhg bvhfg nhhtn nrtn vbhtnvcbhtjngnbc trjhfbbv ghhghhfgbvchg hnjfgjfgjgn hhfhgdhfgdj hgcjgjgfjgj hfhfgjhgj gjhgjgjhjb ghfghfhh hhhvhfdhfh gfhfhfjh hg fhjhfgfjhfgj ghfhfhdfhfdh hfhnfjhfc vhhhh

Suspect Details

Suspect Name	ID Type	Country Code	ID Number
abcd	Email	N/A	abc@gmail.com

Please Upload Any Photograph of Suspect's: N/A

Address for Suspect

House No.	1	Country	INDIA
Street Name	2	State	KERALA
Colony	3	District	THRISSUR RURAL
Vill / Town / City	4	Police Station	PAZHAYANNUR
Tehsil	abc	Pincode	234554

Complainant Details

Name	ABC
Mobile No.	8920244575
Gender.	Male
DOB.	01/07/2019
Father Name :	bcd
Relationship With the Victim	Father
National ID of Victim	Office Lens 20160104-160334__1451903942_107.167.105.54.jpg
Email Id	abc@gmail.com
Nationality :	INDIAN

Address for Correspondence

House No.	N/A	Country	INDIA
Street Name	N/A	State	KARNATAKA
Colony	N/A	District	HAVERI
Vill / Town / City	N/A	Police Station	N/A
Tehsil	N/A	Pincode	N/A

Uploaded File Information:

Number of Uploaded File: 1

(1). File Name :	Shrawan Kumar - Experience Letter.pdf
Binary Hash of File(SHA256) :	E898817278C46D1917B6F4154586C97EE086BAF3300D45E9D944F86D7869602A
Binary Hash of File(MD5) :	2F904C102324592D74D90D1907D7E9E0

Snapshot: Sample of downloaded complaint

5. INFORMATION REQUIRED FOR REPORTING OF CYBERCRIME COMPLAINTS- CATEGORIES/SUB-CATEGORIES

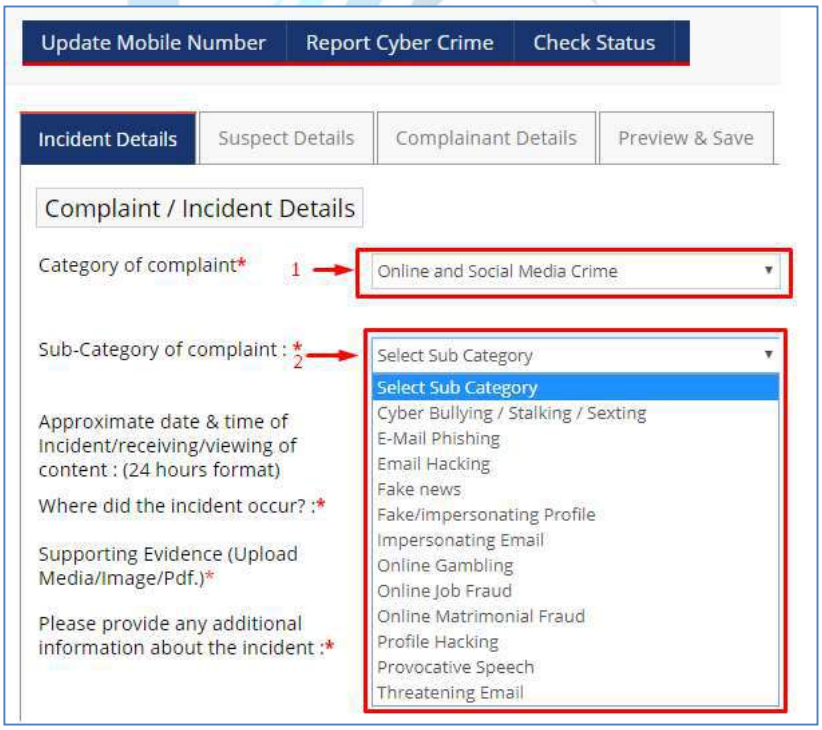
5.1 Report Online and Social Media Related Crime

To report cybercrimes related to social media, Go to homepage, Click on **File a Complaint**→ Read and Accept the **Acknowledgement**→ Select **Report Other Cyber Cime** → Login

After login, under the "**Incident Details**" tab, complainant need to provide the following details:

1. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"

2. Select the "Sub-category of complaint" (Mandatory) from the drop-down (multiple options are availabe in drop-down), select one – ***1.*** *Cyber Bullying/Stalking/Sexting,* ***2.*** *E-Mail Phishing,* ***3.*** *E-mail Hacking,* ***4.*** *Fake/Impersonating Profile,* ***5.*** *Impersonating Email,* ***6.*** *Online Job Fraud,* ***7.*** *Online Matrimonial Fraud,* ***8.*** *Profile Hacking,* ***9.*** *Provocative Speech,* ***10.*** *Intimidating Email.*



5.1.1Cyber Bullying/Stalking/Sexting

Under this sub-category you can report cyber stalking incidents in which attacker uses the internet and other electronic devices to persistently harass the victim. Also, bullying incidents committed using online communication medium like e-mail, social media, SMS, messengers, forums etc., to harass, threaten, embarrass, and humiliate the victim can also be reported. The complainant can

also report any incidence related to sending or receiving of offending sexual words, pictures, or videos via technology, typically a mobile phone.

5.1.1.1 To report a complaint under this sub-category, you may keep following information ready before registering your complaint:

i. If you have received cyberbullying/stalking related SMS:
   a. Take screenshot/s of some SMS, showing the content for upload as evidence
   b. Provide the details of date/time when such SMS have been received for filling in the incident description field

ii. If you have received cyberbullying/stalking related emails:
   a. Save some emails as pdf or .eml files or keep scan of some email prints to be uploaded as evidence
   b. If emails have attachments, then keep attachments ready for upload as evidence

iii. If you are being stalked/bullied on messenger such as WhatsApp, Hike etc.:
   a. Take screen shot of some chats showing the senders number as well as content for upload as evidence
   b. Export such chat to your email (if you have) and save it as .pdf/.eml or take scan of printout of such chat for upload as evidence

iv. If you are being bullied/stalked on social media platform/forums/blogs, such as YouTube, Facebook etc.
   a. Note down the URL (website address) where such content is seen
   b. Save the page showing abusive content or screenshot as a file for uploading as evidence

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, messenger chat, website URL etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B, Section 8.1 and Annexure C, Section 3.1**

5.1.1.2 Complaint reporting

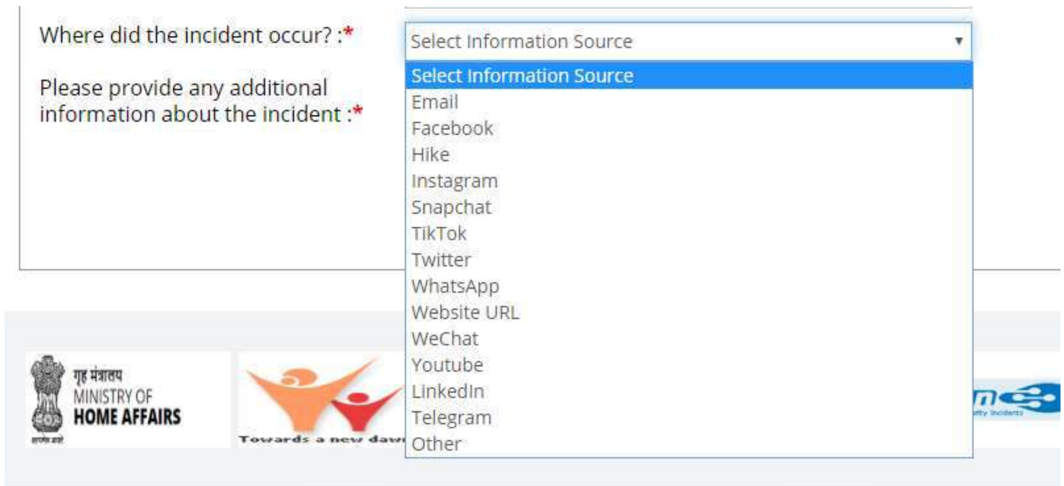
I. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"

II. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Cyber Bullying/Stalking/Sexting"**

III. Select approximate "Date and Time" of incident (Mandatory)

viii. Give "Reason for delay in reporting"

IV. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other. (Mandatory)

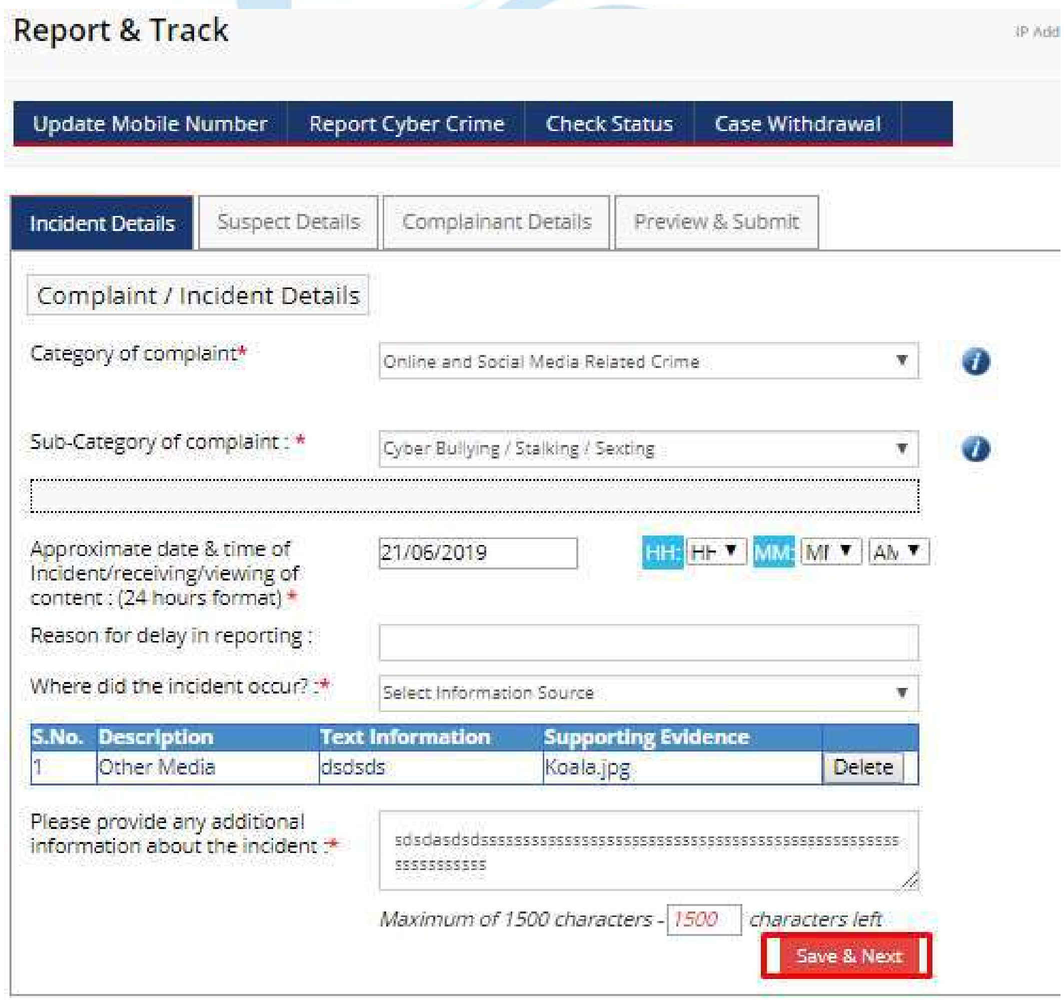


Select the "Where did the incident occur?" please give id related to incident

V. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (**refer to 5.1.1.1**) (Mandatory)

VI. Provide any additional information about the incident.(Mandatory)

VII. Click **Save and Next** to proceed



To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.1.2 E-Mail Phishing

A fraudulent email message designed to be a legitimate person or organization and trick the recipient to share personal information, such as passwords, bank account numbers. Email headers contain a significant amount of information—like digital postmarks—that identify how the message got from the sender to the recipient.

5.1.2.1 To report a complaint under this sub-category, you may keep following information ready before registering your complaint:

If you have received phishing email:

a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
b. Note down/copy the full email headers details of phishing emails (the same is not required if .email has been saved as .eml)
c. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

Note1: You must preserve the original evidence i.e. do not delete emails, email header, screenshot attachments etc., as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B, Section 8.1**

5.1.2.2 Complaint Reporting

i. Select the Category of complaint(Mandatory) from the drop-down "**Online and Social Media Related Crime**"

ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Email Phishing**"

ix. Select approximate "Date and Time" of incident (Mandatory)

x. Give "Reason for delay in reporting"

xi. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other. (Mandatory)

xii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (**refer to 5.1.2.1**) (Mandatory)

VIII. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

xiii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.1.3 Email Hacking

You can report if someone else compromised your Email account and or using it without your permission. Sending you unsolicited/spam mails containing attachments that have malwares embedded in them. Once such emails are opened and attachments activated the malware gets discreetly downloaded and installed on your device. The malware could be a key logger that captures and sends all the keyboard taps to the fraudsters, which includes your account passwords. The other possible malwares could be ones that capture screenshot or read and transmit saved passwords. Email accounts having 2-factor authentication (2FA) can also be got hacked when users share their one-time password (OTP) with fraudsters after getting tricked by social engineering tools.

5.1.3.1 To report a complaint under this sub-category, you may keep following information ready before registering your complaint:

I. If you have received an email hacking related SMS:
   a. Take the screen shot of the SMS (depicting the fraud content) and the same need to be updated on the portal as evidence
   b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

II. If you have received a fraudulent Email:
   a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
   b. Note down/copy the full email Header details of phishing emails (the same is not required if .email has been saved as .eml)
   c. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, screenshots etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.
Note2: For further details on above points you may refer to **Annexure B Help, Section 9**

5.1.3.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"

ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Email Hacking**"

iii. Select approximate "Date and Time" of incident (Mandatory)

iv. Give "Reason for delay in reporting"

v. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other. (Mandatory)

vi. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (**refer to 5.1.3.1**) (Mandatory)

IX. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

vii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.1.4 Fake/Impersonating Profile

You can report an incident wherein a person created your fake profile in any platform and spreads rumors and objectionable content on social media, instant messaging platforms etc. or tries to cheat or defame you or others using fake profile.

5.1.4.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you received or found fake/impersonating profile on internet messaging platform such as WhatsApp, Hike etc.:
   a. Take the screenshot of the profile depicting the fake/impersonating account number, user ID, date and time for uploading the same as evidence on the portal

ii. If you received or found fake/impersonating profile on website/blogs or social media platform/forums such as YouTube, Facebook, twitter etc.
   a. Note down/ copy (to your device/ desktop) the URL or user ID where you have seen such content
   b. Take the screen shot of the page or save the page (as .pdf)showing fake profile on your device/ desktop for uploading the same as an evidence on the portal

Note1: In all above cases, you must preserve the original evidence i.e. do not delete the messenger chats, screenshots, profile ID, URLs etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.2**

5.1.4.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"

ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Fake/Impersonating Profile**"

iii. Select approximate "Date and Time" of incident (Mandatory)

iv. Give "Reason for delay in reporting"

v. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other . (Mandatory)

vi. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.1.5.1) (Mandatory)

X. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

vii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.1.5 Impersonating Email

You can report any incident or person who falsely claim to be someone which he/she is not through a fake email profile on any platform and/or spreads rumors and objectionable content online, social media, instant messaging platforms etc.

5.1.5.1 To report a complaint, you may keep following information ready before registering your complaint:

If you have received an impersonating email:

a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
b. Note down/ copy the full email Header details of phishing emails (the same is not required if .email has been saved as .eml)
c. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

Note1: You must preserve the original evidence i.e. do not delete emails, attachments, screenshot etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.
Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.3**

5.1.5.2 Complaint reporting

I. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"
II. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Impersonating Email"**
III. Service Provider (Mandatory)
IV. Full Header of Email (Mandatory)

V. Select approximate "Date and Time" of incident (Mandatory)
VI. Give "Reason for delay in reporting"

VII. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other. (Mandatory)
VIII. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.1.6.1) (Mandatory)

XI. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

IX. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.1.6 Online Job Fraud

You can report incident involving deceiving you or somebody you know who is seeking employment by giving them the false hope of employment or of earning high salaries or of extra income and cheat you/them by taking money.

5.1.6.1 To report a complaint related to online job fraud, you may keep following information ready before registering your complaint:

i. If you have received job fraud details on SMS:
   a. Take the screenshot/s of the SMS (depicting the content details) and the sender details (name, email, other details) need to be updated on the portal as evidence
   b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

ii. If you have received job fraud email:
   a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
   b. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

iii. If you received or found job fraud related information on social media platform/forums/blogs such as Facebook, Twitter, LinkedIn etc.
   a. Note down/ Copy (to your device/ desktop) the URL where you have seen such content
   b. Provide the other details like user ID, email, contact number, job details etc.
   c. Take the screen shot of the page or save the page (as .pdf) showing content on your device/ desktop for uploading the same as an evidence on the portal

iv. If you lost the money then provide the banking transaction details.

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, screenshots, Website URL etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.
Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.4**

5.1.6.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"

ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Online Job Fraud"**

iii. Select approximate "Date and Time" of incident (Mandatory)

iv. Give "Reason for delay in reporting"

v. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other . (Mandatory)

X. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.1.8.1) (Mandatory)

vi. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

vii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.1.7 Online Matrimonial Fraud

You can report any incident where fraudsters create fake profiles on leading matrimonial websites for cheating.

5.1.7.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you have received matrimonial fraud related details on SMS:
   a. Take the screenshot/s of the SMS (depicting the content details) and the sender details (name, email, other details) need to be updated on the portal as evidence
   b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

ii. If you have received matrimonial fraud related details on E-mail:
   a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
   b. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

iii. If you received or found online matrimonial fraud related content on social media platform/forums/blogs such as Facebook, twitter, LinkedIn etc.
   a. Note down/ Copy (to your device/ desktop) the URL where you have seen such content
   b. Provide the other details like user ID, email, contact number, matrimonial details etc.
   c. Take the screen shot of the page or save the page (as .pdf) showing content on your device/ desktop for uploading the same as an evidence on the portal

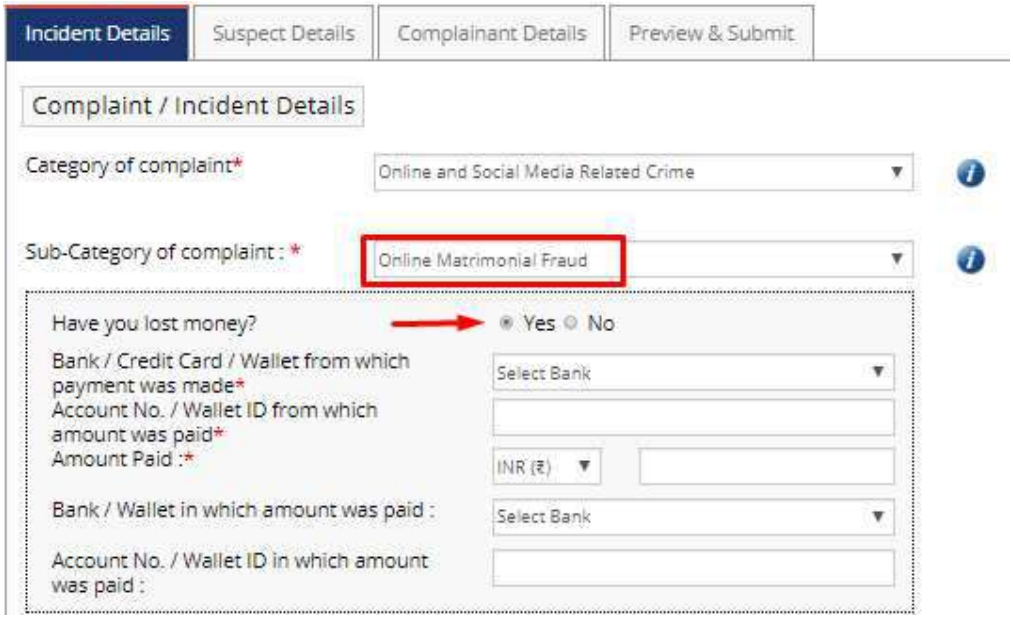
iv. If you lost the money then provide the banking transaction details, bank account, transaction details, suspect address, company name, website URL, email id, mobile no, or any information of the platform source where incident has happened.

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, screenshots, Website URL etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.5**

5.1.7.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Online Matrimonial Fraud"**
iii. Have you lost money? (Select Yes or No) If **Yes** then fill the below details
iv. Bank Name from which payment was made (Mandatory)
v. Account No. from which amount was paid (Mandatory)
vi. Amount Paid (Mandatory)
vii. Bank in which amount was paid
viii. Account no. in which amount was paid



ix. Select approximate "Date and Time" of incident (Mandatory)

x. Give "Reason for delay in reporting"

xi. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

xii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.1.9.1) (Mandatory)

xiii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

xiv. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.1.8 Profile Hacking

You can report if someone else compromised your social media account and or using it without your permission.

5.1.8.1 To report a complaint under this sub-category user should have details like website name, URL of the profile, Email id, Mobile no, User ID or any information of the platform source where incident has happened. Following are some example of profile URL:

Facebook ID: https://www.facebook.com/profile.php?id=1000000653286827
Twitter ID: @username
Instagram: @Username
WhatsApp: +91-9560348XXX

Note: For further details on above points you may refer to **Annexure B Help**

5.1.8.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"

ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Profile Hacking"**

iii. Select approximate "Date and Time" of incident (Mandatory)

iv. Give "Reason for delay in reporting"

v. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

vi. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.1.10.1) (Mandatory)

vii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

viii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.1.9 Provocative Speech

To report a complaint under this sub-category user should have details like website name, URL of the profile, Email id, Mobile no, User ID or any information of the platform source where incident has happened.

5.1.9.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you have received any provocative speech related link details through SMS:
   a. Take the screenshot/s of the SMS (depicting the objectionable content) and sender's details (number or ID) the same need to be updated on the portal as evidence
   b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

ii. If you received or found provocative speech details on messaging platform such as WhatsApp, Hike, Instagram etc.:
   a. Take the screenshot/s of the chats depicting the content with sender's number along with date and time for uploading the same as evidence on the portal

iii. If you received or found provocative speech on social media platform/forums/blogs such as YouTube, Facebook, Twitter etc.
   a. Note down/ Copy (to your device/ desktop) the URL or user ID where you have seen such content
   b. Take the screen shot of the page or save the page (as .pdf) showing abusive content on your device/ desktop for uploading the same as an evidence on the portal

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, messenger Chats, website URL, screenshots etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

5.1.9.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"

ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Provocative Speech"**

iii. Select approximate "Date and Time" of incident (Mandatory)

iv. Give "Reason for delay in reporting"

v. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

vi. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.1.11.1) (Mandatory)

vii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

viii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.1.10 Intimidating Email

You can report if someone threatening you through e-mail.

5.1.10.1 To report a complaint, you may keep following information ready before registering your complaint:

If you have received threatening email:

a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
b. Note down/ copy the full email Header details of phishing emails (the same is not required if .email has been saved as .eml)
c. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

Note1: You must preserve the original evidence i.e. do not delete emails, attachment, SMS, screenshots etc., as these could be needed by law enforcement agency as evidence for prosecuting the offender.
Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.6**

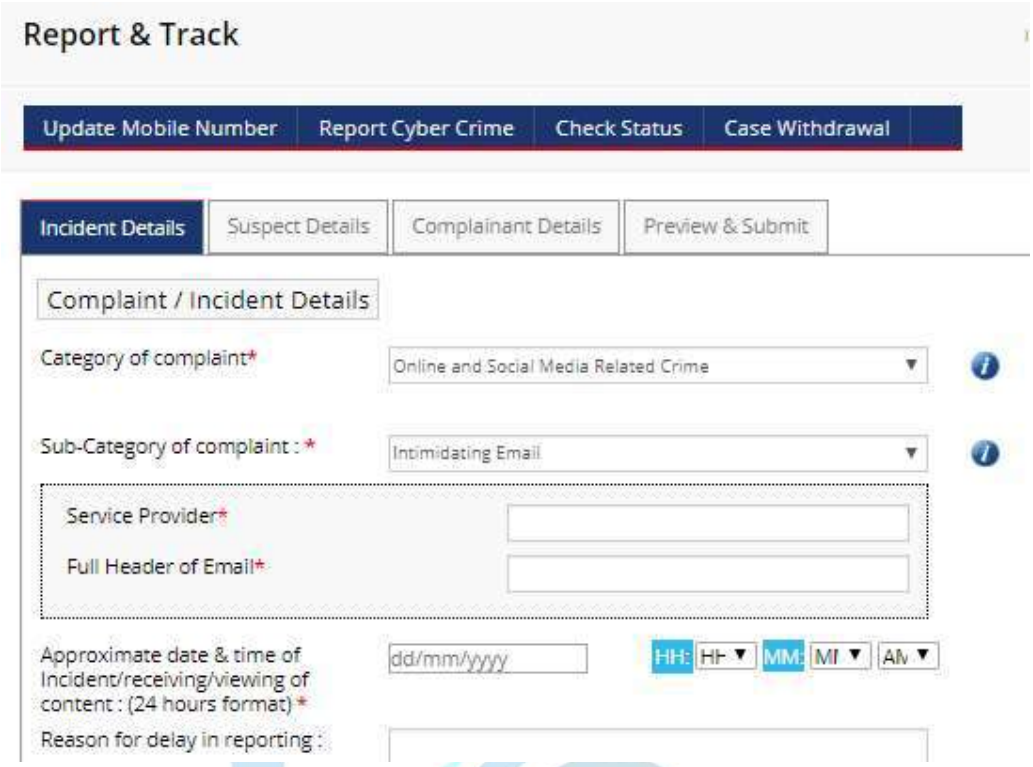
5.1.10.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online and Social Media Related Crime**"

ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Intimidating Email"**

iii. Enter service provider (Mandatory)

iv. Enter full header of Email (Mandatory)



v. Select approximate "Date and Time" of incident (Mandatory)

vi. Give "Reason for delay in reporting"

vii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.1.12.1) (Mandatory)

viii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

ix. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.2 Report Online Financial Fraud

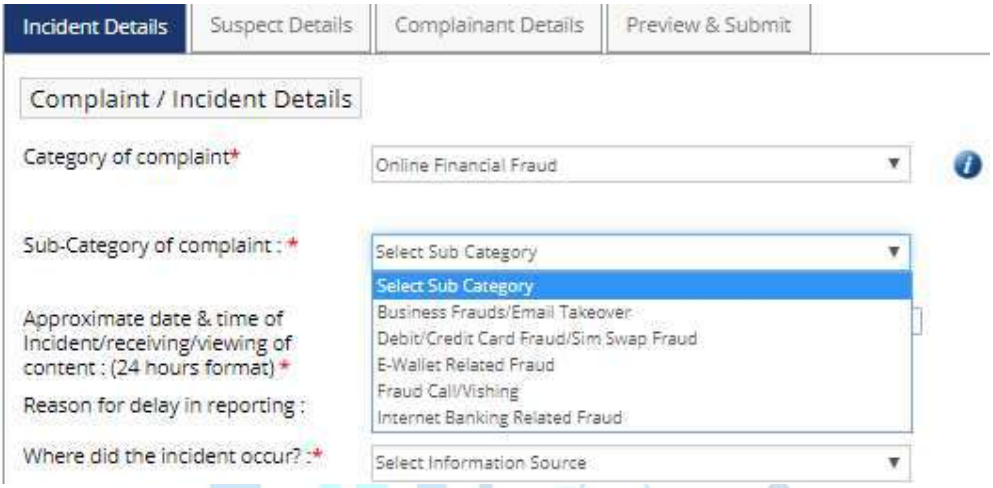
If any unknown person had withdrawn money/ made transactions through your internet banking, credit/debit cards, Wallets or UPI you can report such incidents.
To report a complaint under online financial fraud category user should have following details mandatory:

- Bank statement from the concerned bank.
- Make a copy of SMSs received related to the alleged transactions.
- Copy of your ID proof and address proof as shown in the bank records.

Go to homepage, Click on **File a Complaint**→ Read and Accept the **Acknowledgement**→ Select **Report Other Cyber Cime** → Login

Provide the details as required for complaint reporting under "**Incident Details**"

1. Select the "Category of complaint" (Mandatory) from the drop-down "**Online Financial Fraud**"
2. Select the "Sub-category of complaint" (Mandatory) from the drop-down (5 options are availabe in drop-down – ***1.*** *Business Frauds/Email Takeover,* ***2.*** *Debit/Credit Card Frauds/SIM Swap Fraud,* ***3.*** *E-Wallet Related Fraud,* ***4.****Fraud Call/Vishing,* ***5.*** *Internet Banking Related Fraud*



5.2.1 Business Frauds/Email Takeover

You can report Business e-mail compromise or take over using which monetary frauds have been committed.

5.2.1.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you have received business related fraud SMS:
   a. Take the screenshot/s of the SMS (depicting the content details) and the sender details (name, other details) need to be updated on the portal as evidence
   b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

ii. If you have received a business-related fraud email:
   a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
   b. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

iii. If you received or found any business-related fraud contents on social media platform/forums/blogs such as Facebook, twitter, LinkedIn etc.
   a. Note down/ Copy (to your device/ desktop) the URL where you have seen such content

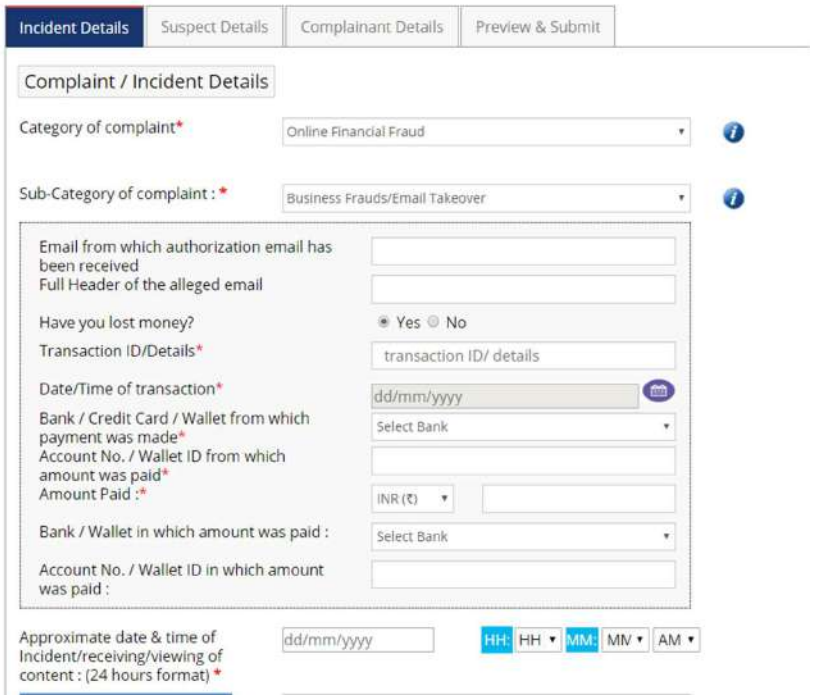
b. Provide the other details like user ID, email, contact number, job details etc.
c. Take the screen shot of the page or save the page (as .pdf) showing content on your device/ desktop for uploading the same as an evidence on the portal

iv. If you lost the money then provide the banking transaction details, bank account, transaction details, suspect address, company name, website URL, email id, mobile no, or any information of the platform source where incident has happened.

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, screenshots, Website URL etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.
Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.7**

5.2.1.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online Financial Fraud"**
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Business Frauds/Email Takeover"**
iii. Email from which authorization email has been received
iv. Full Header of the alleged email
v. Have you lost money? (Select Yes or No)If **Yes** then fill the below details
vi. Transaction ID/Details (Details about the transaction ID/reference no eg. 877687263) (Mandatory)
vii. Date/Time of transaction dd/mm/yyyy (Mandatory)
viii. Bank Name from which payment was made (Mandatory)
ix. Account No. from which amount was paid (Mandatory)
x. Amount Paid(Mandatory)
xi. Bank in which amount was paid
xii. Account no. in which amount was paid



xiii. Select approximate "Date and Time" of incident (Mandatory)

xiv. Give "Reason for delay in reporting"

xv. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

xvi. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.2.1.1) (Mandatory)

xvii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

xviii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.2.2 Debit/Credit Card Fraud/SIM Swap Fraud

You can report any fraudulent online transaction in your bank account through debit or credit card without your knowledge.

5.2.2.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you have received financial debit/credit card fraud transaction related SMS:
   a. Take a screenshot/s or copy of SMSs received related to the alleged transactions and upload this as evidence
   b. Details of date/time when such SMS have been received for filling in the incident description field

ii. If you have received financial debit/credit card fraud transaction related emails:

a. Save some emails as pdf or .eml files or keep scan of some email prints to be uploaded as evidence ii) If emails have attachments, then keep attachments ready for uploading as evidence

iii. If you have received SIM swap related call or SMS
   a. Take a screenshot/s or copy of Number and SMSs received related to the alleged transactions and upload this as evidence

iv. If you lost the money then provide the screenshot/s or copy details of banking transaction details, bank account, transaction details, suspect address, company name, website URL, email id, mobile no, or any information of the platform source where incident has happened.

v. Provide the screenshot/s or copy of the last six months bank statement from your concerned bank account.

vi. Provide the screenshot/s or copy of your ID proof and address proof as shown in the bank records.

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, contact number, screenshots etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.8**

5.2.2.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online Financial Fraud"**

ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Debit/Credit Card Fraud/SIM Swap Fraud"**

iii. Have you lost money? (Select Yes or No)If **Yes** then fill the below details

iv. Transaction ID/Details (Details about the transaction ID/reference no eg. 877687263) (Mandatory)

v. Date/Time of transaction dd/mm/yyyy (Mandatory)

vi. Bank Name from which payment was made (Mandatory)

vii. Account No. from which amount was paid (Mandatory)

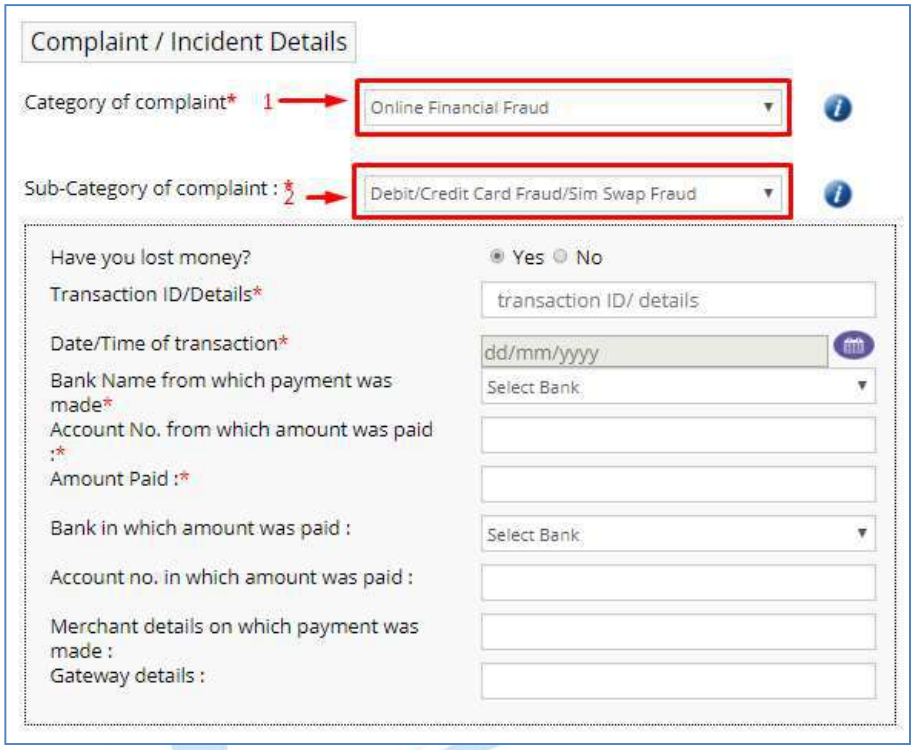
viii. Amount Paid (Details about lost amount)(Mandatory)

ix. Bank in which amount was paid

x. Account no. in which amount was paid

xi. Merchant details on which payment was made

xii. Gateway details (Payment gateway information)



xiii. Select approximate "Date and Time" of incident (Mandatory)

xiv. Give "Reason for delay in reporting"

xv. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other . (Mandatory)

xvi. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.2.2.1) (Mandatory)

xvii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

xviii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.2.3 E-Wallet Related Fraud

You can report any fraudulent online transaction in E-Wallet which is being charged to you and occurred without your knowledge. Wallet summary showing the details of fraudulent transactions. Our wallet has option to save transaction history which can be uploaded as evidence to show fraudulent transactions.

5.2.3.1 To report a complaint, you may keep following information ready before registering your complaint:

I. If you have received e-wallet fraud transaction on your email

a. You can save details of wallet transactions email of such transactions as .pdf/.eml file and keep it ready for uploading as evidence

II. Provide the screenshot/s or copy of your ID proof and address proof as shown in the bank records.

Note1: You must preserve the original evidence i.e. do not delete transaction history in your mobile as well as emails (if received) as these could be needed by law enforcement agency as evidence for investigation and prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.9**

5.2.3.2 Complaint Reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online Financial Fraud"**

ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**E-Wallet Related Fraud"**

iii. Have you lost money? (Select Yes or No)If **Yes** then fill the below details

iv. Name of wallet (Mandatory)

v. Transaction ID/Details (Details about the transaction ID/reference no eg. 877687263) (Mandatory)

vi. Date/Time of transaction dd/mm/yyyy (Mandatory)

vii. Bank Name from which payment was made

viii. Account No. from which amount was paid

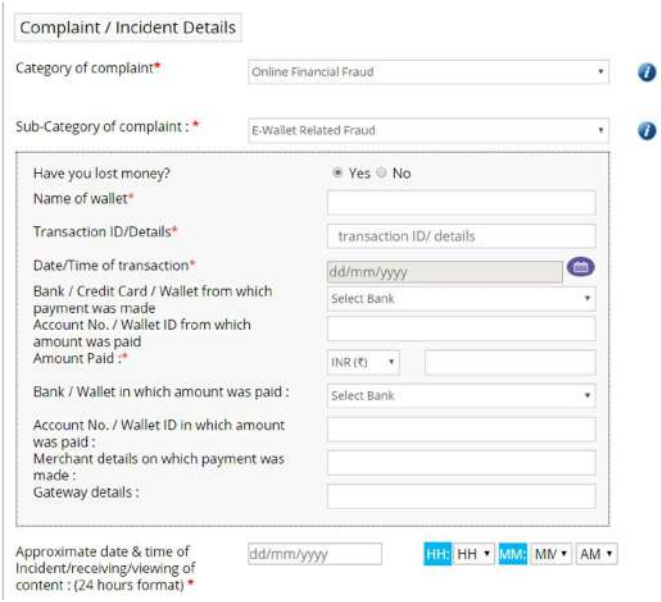
ix. Amount Paid (Details about lost amount)(Mandatory)

x. Bank in which amount was paid

xi. Account no. in which amount was paid

xii. Merchant details on which payment was made

xiii. Gateway details (Payment gateway information)



xiv. Select approximate “Date and Time” of incident (Mandatory)

xv. Give “Reason for delay in reporting”

xvi. Select the “Where did the incident occur?”- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

xvii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.2.3.1) (Mandatory)

xviii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

xix. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.2.4 Fraud Call/Vishing

Several instances have occurred wherein people receive phone calls that appear to be from their bank. The caller usually pretends to be a bank representative or someone from the bank’s technical team. In most cases, the caller sounds professional and provides a convincing reason for calling the customer. You may get unexpected prize scams include lottery scams, fake scams and travel scams call.

You can report any fraudulent call incident which is an attempt where fraudsters try to seek your personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

5.2.4.1 To report a complaint, you may keep following information ready before registering your complaint:

i. Provide the fraud callers number details

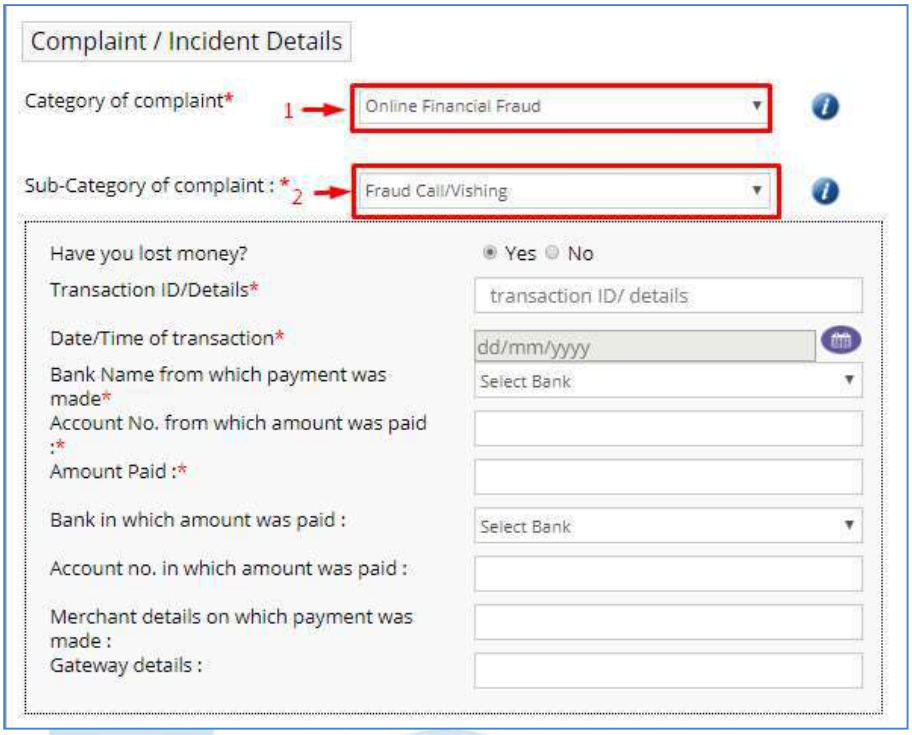
ii. If you received internet based fraud or vishing call, take the screenshot/s of the sender's number along with date and time for uploading the same as evidence on the portal
iii. In case, if you are having the call recording, then uploading the same as evidence on the portal. (Audio file format like .amr .3gp .wav or similar)
iv. If you lost the money then provide the screenshot/s or copy details of banking transaction details, bank account, transaction details, suspect address, company name, website URL, email id, mobile no, or any information of the platform source where incident has happened.

Note1: In all above cases, you must preserve the original evidence i.e. do not delete call details, numbers, call recordings, email etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.10**

5.2.4.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online Financial Fraud"**
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Fraud Call/Vishing"**
iii. Have you lost money? (Select Yes or No)If **Yes** then fill the below details
iv. Transaction ID/Details (Details about the transaction ID/reference no eg. 877687263) (Mandatory)
v. Date/Time of transaction dd/mm/yyyy (Mandatory)
vi. Bank Name from which payment was made (Mandatory)
vii. Account No. from which amount was paid (Mandatory)
viii. Amount Paid (Details about lost amount)(Mandatory)
ix. Bank in which amount was paid
x. Account no. in which amount was paid
xi. Merchant details on which payment was made
xii. Gateway details (Payment gateway information)



xiii. Select approximate "Date and Time" of incident (Mandatory)

xiv. Give "Reason for delay in reporting"

xv. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

xvi. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.2.4.1) (Mandatory)

xvii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

xviii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.2.5 Internet banking Related Fraud

It is a fraud or theft committed using online technology to illegally remove money from a bank account and/or transfer money to an account in a different bank. You can report any fraudulent online transaction in your bank account through internet banking/Mobile App without your knowledge.

5.2.5.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you have received fraudulent transaction SMS:
   a. Take the screenshot/s of the SMS (depicting the content details) and the sender details (name, other details) need to be updated on the portal as evidence

b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

ii. If you have received an internet banking related fraud email:
   a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
   b. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

iii. If you were duped of your money through a link or content available on social media platform/forums/blogs such as Facebook, twitter, LinkedIn etc.
   a. Note down/ Copy (to your device/ desktop) the URL where you have seen such content
   b. Provide the other details like user ID, email, contact number, job details etc.
   c. Take the screen shot of the page or save the page (as .pdf) showing content on your device/ desktop for uploading the same as an evidence on the portal

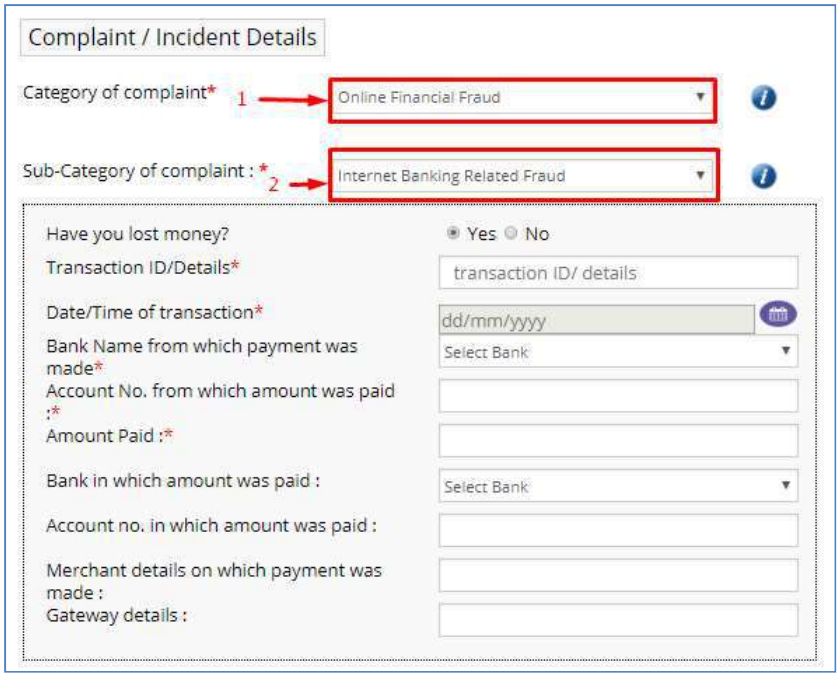
iv. If you lost the money then provide the screenshot/s or copy details of banking transaction details, bank account, transaction details, suspect address, company name, website URL, email id, mobile no, or any information of the platform source where incident has happened.

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, attachments transactions details, screenshots, Website URL etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.11**

5.2.5.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online Financial Fraud"**
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Internet banking Related Fraud"**
iii. Have you lost money? (Select Yes or No)If **Yes** then fill the below details
iv. Transaction ID/Details (Details about the transaction ID/reference no eg. 877687263) (Mandatory)
v. Date/Time of transaction dd/mm/yyyy (Mandatory)
vi. Bank Name from which payment was made (Mandatory)
vii. Account No. from which amount was paid (Mandatory)
viii. Amount Paid (Details about lost amount)(Mandatory)
ix. Bank in which amount was paid
x. Account no. in which amount was paid
xi. Merchant details on which payment was made
xii. Gateway details (Payment gateway information)



xiii. Select approximate "Date and Time" of incident (Mandatory)

xiv. Give "Reason for delay in reporting"

xv. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

xvi. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.2.5.1) (Mandatory)

xvii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

xviii. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.3 Report Ransomware

It is a type of computer malware that locks your data on communication devices such as desktops, Laptops, Mobile phones etc., holding data/information as a hostage. You will be asked to pay the demanded ransom in some cryptocurrency (Bitcoin, ripple etc.) to get your device unlocked. Bitcoin is a cryptocurrency, a form of electronic cash or virtual money. There is no guarantee that your data will be unlocked after paying the ransom.

5.3.1 Ransomware

To report a complaint, you may keep following information ready before registering your complaint:

i. Provide the screenshot/s copy or the details like Bitcoin details, Email id /phone number or any other means of communication through which ransom has been demanded, ransom amount, or any information of the platform source where incident has happened.

ii. If you have received ransom email:
   a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
   b. Note down/ copy the full email Header details of phishing emails (the same is not required if .email has been saved as .eml)
   c. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

Note1: In all above cases, you must preserve the original evidence i.e. do not delete emails, attachments etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.12**

5.3.1.1 Complaint reporting

Go to homepage, Click on **File a Complaint**→ Read and Accept the **Acknowledgement**→ Select **Report Other Cyber Crime** → Login

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Ransomware**
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Ransomware"**
iii. Bitcoin Address/Details (Provide the alleged payment address details) (Mandatory)
iv. Darknet ID/ Details (Ex. website, emailID) (Mandatory)

v. Select approximate "Date and Time" of incident (Mandatory)
vi. Give "Reason for delay in reporting"
vii. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)
viii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.3.1) (Mandatory)
ix. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)
x. Click on **Save and Next** to proceed

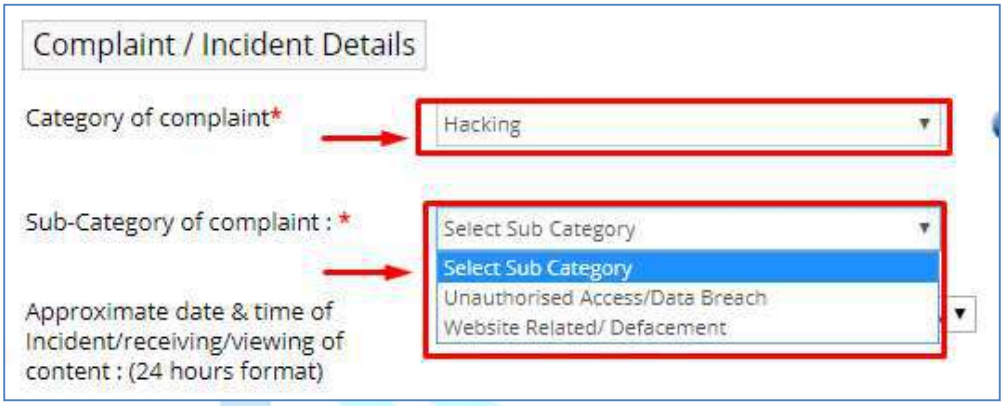
To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.4 Report Hacking

It is an attempt to exploit weaknesses for gaining unauthorized access in a computer system or network.
Go to homepage, Click on **File a Complaint**→ Read and Accept the **Acknowledgement**→ Select **Report Other Cyber Cime** → Login

Provide the details as required for complaint reporting under "**Incident Details**"

1. Select the "Category of complaint" (Mandatory) from the drop-down "**Hacking**"
2. Select the "Sub-category of complaint" (Mandatory) from the drop-down (2 options are availabe in drop-down – ***1.*** *Unauthorised Access/Data Breach,* ***2.*** *Website Related/Defacement*



5.4.1 Unauthorized Access/Data Breach

You can report any incidents of any person accessing your computer, mobile website, server etc., without your permission.

5.4.1.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you have received hacking related SMS:
   a. Take the screenshot/s of the SMS (depicting the illegal details) and the sender details (name, other details) need to be updated on the portal as evidence
   b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

ii. If you have received an email related to hacking, data theft:
   a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
   b. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

iii. If you received or found any details related to hacking, data breached on a website:

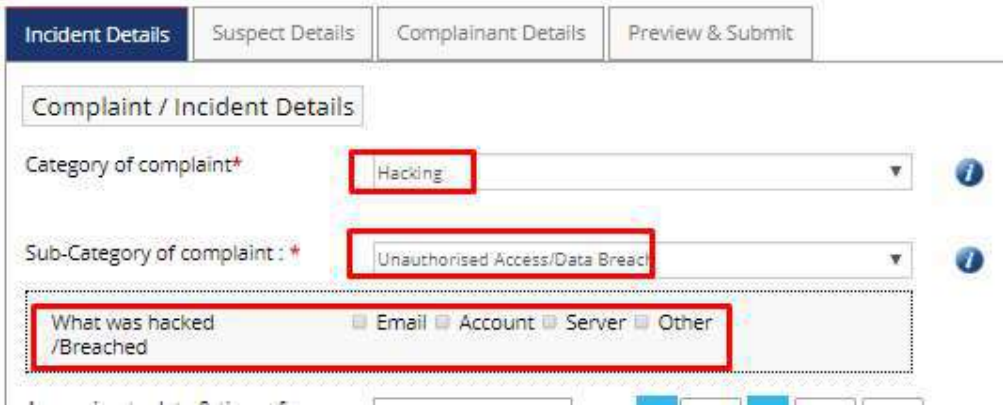
a. Note down/ Copy (to your device/ desktop) the URL where you have seen such content
b. Take the screen shot of the page or save the page (as .pdf) showing content on your device/ desktop for uploading the same as an evidence on the portal

iv. Provide the screenshots or copy of the details like what was hacked e.g. website URL, Account, Server, email or any information of the platform source where incident has happened.

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, attachment, mobile no, website URL, messenger chat, screenshot etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.
Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.13**

5.4.1.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Hacking"**
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Unauthorised Access/Data Breach"**
iii. Select "Mode of communication" and provide details (e.g. Email, Account, Server, Other)



iv. Select approximate "Date and Time" of incident (Mandatory)
v. Give "Reason for delay in reporting"
vi. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)
vii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.4.1.1) (Mandatory)
viii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)
ix. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.4.2 Website Related/Defacement

You can report a complaint related to website defacement. Website defacement is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of hackers, who break into a web server and replace the hosted website with one of their own.

5.4.2.1 To report a complaint, you may keep following information ready before registering your complaint:

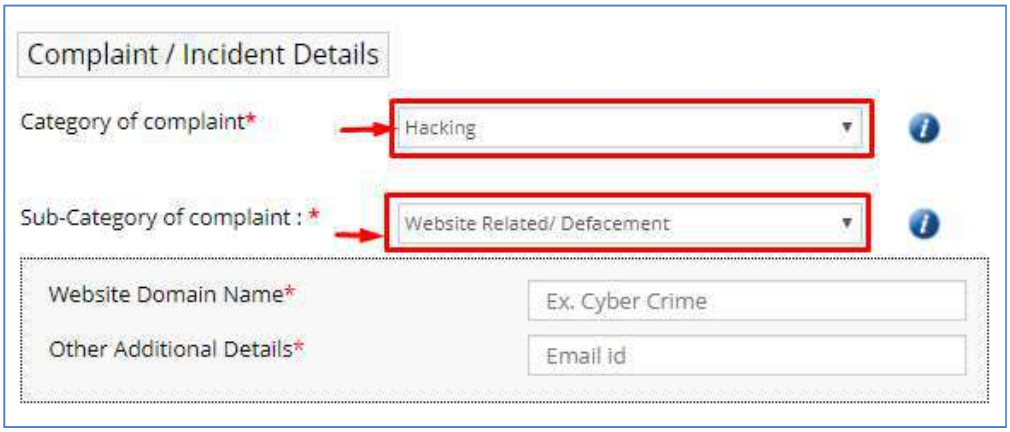
i. Provide the details URL of defaced or hacked website
ii. If you received or found website defacement/hacked information on media platform/forums/blogs such as Facebook, Twitter, LinkedIn etc.
    a. Note down/ Copy (to your device/ desktop) the URL where you have seen such content
    b. Provide the details like user ID, email or other
    c. Take the screen shot of the page or save the page (as .pdf) showing content on your device/ desktop for uploading the same as an evidence on the portal

Note1: In all above cases, you must preserve the original evidence i.e. do not delete website URL, hacked mirror URL, messenger Chat etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.14**

5.4.2.2 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Hacking"**
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Website Related/Defacement"**
iii. Website Domain name (Enter the website or URL) (Mandatory)
iv. Other Additional Details (Mandatory)



v. Select approximate "Date and Time" of incident (Mandatory)

vi. Give “Reason for delay in reporting”

vii. Select the “Where did the incident occur?”- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

viii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.4.2.1) (Mandatory)

ix. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

x. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.5 Report Cryptocurrency Crime

Crypto currency is created by solving a complex mathematical problem. RBI has not given any license/authorization to any entity/company to deal with any virtual currency. In the absence of a legal framework, it is not advisable for citizens to deal with virtual currencies such as Bitcoin, Ripple, and Lite coin etc. The legal framework regarding crypto-currencies is yet to be laid down.

These currencies are normally used by criminals operating on the dark web or the hidden web. Legal, bonafide businesses do not normally use Bitcoin. Therefore, any request for business transaction in Bitcoin should raise suspicious and should be avoided

5.5.1 Cryptocurrency Related Fraud

You can report any crypto currency related frauds here. Provide the complete facts in brief about the incident.

5.5.1.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you have received cryptocurrency fraudulent SMS:
   a. Take the screenshot/s of the SMS (depicting the content details) and the sender details (name, other details) need to be updated on the portal as evidence
   b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

ii. If you have received an E-mail:
   a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
   b. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal

iii. Provide the screenshots or copy of the details like what was hacked e.g. website URL, Bitcoin address, wallet details, amount of Bitcoin involved or any information of the platform source where incident has happened.

iv. Provide the address from/to whom purchase/sale of Bitcoin is done

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, website details, wallet details etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.15**

5.5.1.2 Complaint reporting

Go to homepage, Click on **File a Complaint**→ Read and Accept the **Acknowledgement**→ Select **Report Other Cyber Cime** → Login

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Cryptocurrency Crime"**
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Cryptocurrency Fraud"**
iii. Bitcoin Address/Details (Provide the alleged payment address details) (Mandatory)
iv. Darknet ID/ Details (Ex. website, emailID) (Mandatory)

v. Select approximate "Date and Time" of incident (Mandatory)
vi. Give "Reason for delay in reporting"
vii. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)
viii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.4.2.1) (Mandatory)
ix. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)
x. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.6 Report Online Trafficking

Connecting over social media to make business connections, or buy legal goods or services may be perfectly legitimate. However, connecting over social media to buy drugs, or other regulated, controlled or banned products is probably illegal. You can report any forms of trafficking committed using the cyberspace e.g. victim's recruitment, advertising trafficking such as women, children's, laborer's, child pornography, selling of organs, drugs etc.

5.6.1 Online Trafficking

You can report incidents involving trafficking of women, children, men, drugs, weapons etc. wherein online/internet is being used. To report a complaint under this sub-category user should have details like what is being trafficked, website URL, contact details, email or any information of the platform source where incident has happened.

5.6.1.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you received or found online illegal trafficking on messaging platform such as WhatsApp, Hike etc.:
   a. Take the screenshot/s of the chats depicting the content with sender's number along with date and time for upload the same as evidence on the portal
ii. If you received or found online illegal activity on social media platform/forums/blogs such as YouTube, Facebook, Instagram, Twitter etc.
   a. Note down/ Copy (to your device/ desktop) the URL or user ID where you have seen such content
   b. Take the screen shot of the page or save the page (as .pdf) showing abusive content on your device/ desktop for upload the same as an evidence on the portal

Note1: In all above cases, you must preserve the original evidence i.e. do not, messenger Chats, screenshots, website URL etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.
Note2: For further details on above points you may refer to **Annexure B and Annexure C Section 3.16**

5.6.1.2 Complaint reporting

Go to homepage, Click on **File a Complaint**→ Read and Accept the **Acknowledgement**→ Select **Report Other Cyber Cime** → Login

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online Trafficking"**
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Online Trafficking"**
iii. What is being trafficked (women, children, men, drugs, weapons etc.)
iv. Social Media Used (Mandatory)
v. Darknet ID/ Details (Ex. website, emailID)

vi. Select approximate “Date and Time” of incident (Mandatory)

vii. Give “Reason for delay in reporting”

viii. Select the “Where did the incident occur?”- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

ix. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.6.1.1) (Mandatory)

x. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

xi. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.7 Report Online Gambling

5.7.1 Online Gambling

To report a complaint under this category user should have details like illegal online gambling details, website URL and if complainant has lost the money then he/she may provide the banking transaction details.

5.7.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you have received illegal online gambling link through SMS:
   a. Take the screenshot/s of the SMS (depicting the objectionable content) and sender’s details (number or ID) the same need to be updated on the portal as evidence
   b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

ii. If you have received or found illegal online gambling content on messaging platform such as WhatsApp, Hike etc.:
   a. Take the screen shot of the chats depicting the gambling content details with sender’s details (number or ID) along with date and time for uploading the same as evidence on the portal

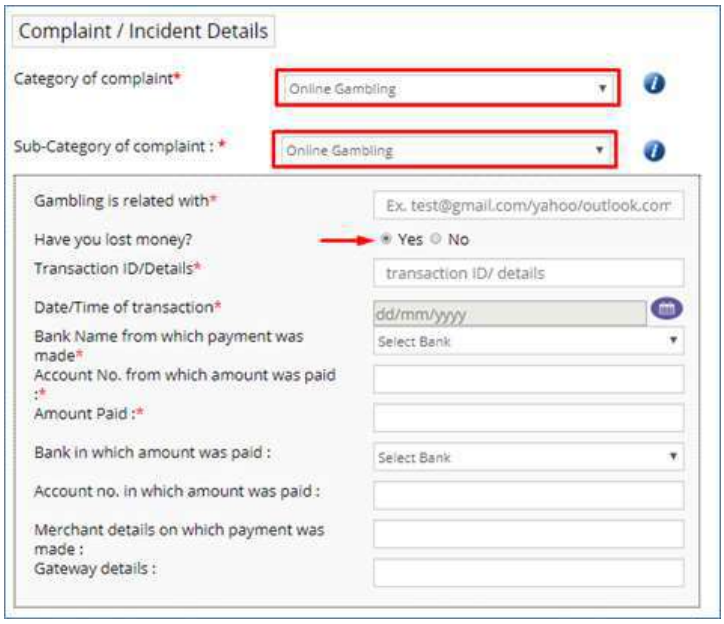
iii. If you have received or found content related illegal online gambling on social media platform/forums/blogs such as YouTube, Facebook, twitter etc.
   a. Note down/ Copy (to your device/ desktop) the URL or user ID where you have seen such content
   b. Take the screen shot of the page or save the page (as .pdf) showing content on your device/ desktop for uploading the same as an evidence on the portal

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, messenger Chats, screenshots etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.

Note2: For further help on above points, refer to **Annexure B Help**

5.7.1.1 Complaint reporting

i. Select the "Category of complaint" (Mandatory) from the drop-down "**Online Gambling**"
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Online Gambling"**
iii. Gambling is related with (Ex. Poker, Betting, casino etc.) (Mandatory)
iv. Have you lost money? (Select Yes or No) If **Yes** then fill the below details
v. Transaction ID/Details(Details about the transaction ID/reference no eg. 877687263) (Mandatory)
vi. Date/Time of transaction dd/mm/yyyy (Mandatory)
vii. Bank Name from which payment was made (Mandatory)
viii. Account No. from which amount was paid (Mandatory)
ix. Amount Paid (Mandatory)
x. Bank in which amount was paid
xi. Account no. in which amount was paid
xii. Merchant details on which payment was made
xiii. Gateway details



xiv. Select approximate “Date and Time” of incident (Mandatory)

xv. Give “Reason for delay in reporting”

xvi. Select the “Where did the incident occur?”- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)

xvii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.1.7.1) (Mandatory)

xviii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)

xix. Click on **Save and Next** to proceed

To proceed with next stage of complaint reporting refer to Step 5 under How to Report A Complaint

5.8 Report Any Other Cyber Crime

If you find that your complaint does not fall under any of the listed categories/sub-categories, report your complaint under this category and sub-category.

5.8.1 To report a complaint, you may keep following information ready before registering your complaint:

i. If you have received cybercrime related information on SMS:
   a. Take the screenshot/s of the SMS (depicting the objectionable content) and sender details (name, ID) same need to be updated on the portal as evidence
   b. Note the date and time when you have received the SMS and same need to be updated in the Incident description field while you report your complaint on the portal

ii. If you have received an email related to cybercrime:
    a. Save the received e-mails in pdf or .eml format or take the screenshot/s of the received e-mail and the same needs to be uploaded on the portal as evidence
    b. If the received e-mails had an attachment/s, then keep the attachment/s ready on your desktop/ device for updating the same as an evidence on the portal
iii. If you received or found cybercrime related content on messaging platform such as WhatsApp, Hike, Skype etc.:
    a. Take the screenshot/s of the chats depicting the objectionable content with sender's number along with date and time for uploading the same as evidence on the portal
iv. If you received or found cybercrime related contents on social media platform/forums/blogs such as YouTube, Facebook, etc.
    a. Note down/ Copy (to your device/ desktop) the URL where you have seen such content
    b. Take the screen shot of the page or save the page (as .pdf) showing abusive content on your device/ desktop for uploading the same as an evidence on the portal

Note1: In all above cases, you must preserve the original evidence i.e. do not delete SMSs, emails, attachment, messenger Chats, website URLS, screenshots etc. as these could be needed by law enforcement agency as evidence for prosecuting the offender.
Note2: For further details on above points you may refer to **Annexure B and Annexure C Sections**

5.8.2 Complaint reporting

Go to homepage, Click on **File a Complaint**→ Read and Accept the **Acknowledgement**→ Select **Report Other Cyber Cime** → Login

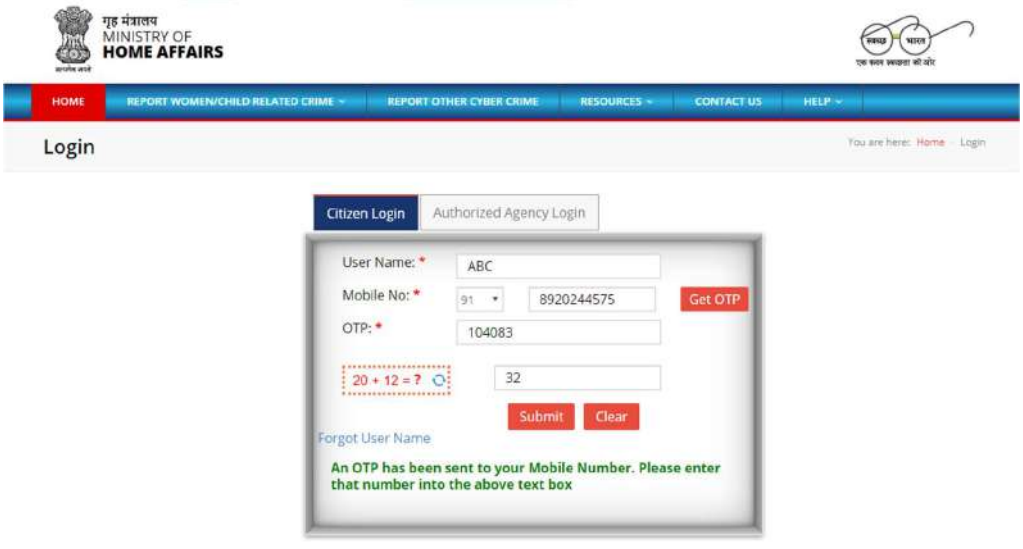
i. Select the "Category of complaint" (Mandatory) from the drop-down "**Any Other Cyber Crime**
ii. Select the Sub-category of complaint (Mandatory) from the drop-down – "**Other"**
iii. Provide Other Crime Details (Mandatory)
iv. Select approximate "Date and Time" of incident (Mandatory)
v. Give "Reason for delay in reporting"
vi. Select the "Where did the incident occur?"- Select from the dropdown the source of evidence like social media platform (Facebook, Twitter, Instagram etc.), messaging platform (WhatsApp, Hike etc.), e-mail, website, URL or other (Mandatory)
vii. Upload evidence (Maximum allowable limit is 5 MB) as applicable. (Refer to 5.7.1) (Mandatory
viii. Provide any additional information about the incident (which you think can be included in the complaint and could help in investigation). (Mandatory)
ix. Click on **Save and Next** to proceed

6. TRACK COMPLAINT STATUS

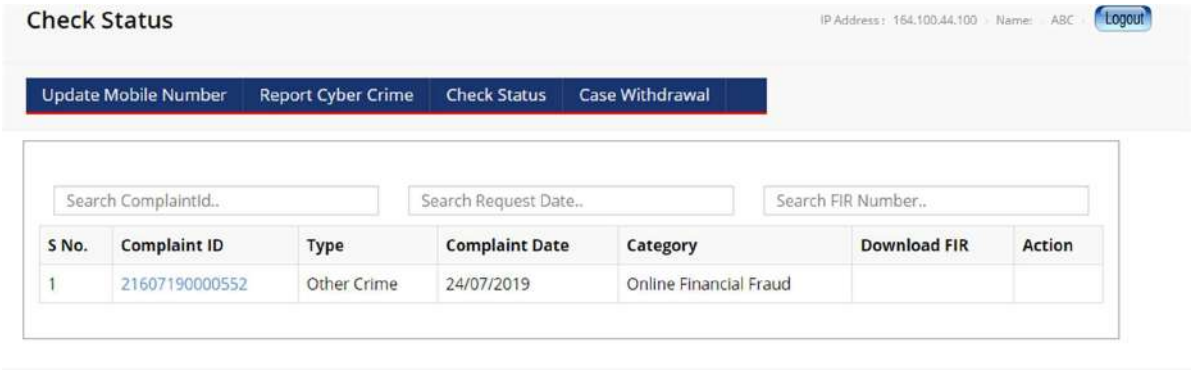
In case you want to **Track the status** of your complaint. Go to homepage, Click on **File a Complaint**→ Read and Accept the **Acknowledgement**→ Select **Report Other Cyber Cime** →**Login** with registered user name & number

a. You need to fill the following details (Mandatory) to login into the system

i. Provide User Name – which is given during reporting the complaint (Mandatory)
ii. Enter your Mobile Number (that you have entered while registering the complaint) (Mandatory)
iii. Enter OTP (received on mobile number) (Mandatory)
iv. Type security answer for authentication
v. Click **Submit** button



b. 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 and email



7. ADDITONAL FEATURES

7.1 Recover Your Username

If You are forget your username, follow the following steps

i. Go to login page and click on "**Forget User name**"
ii. Enter Registered Mobile Number (Mandatory)
iii. Type security answer for authentication
iv. Click **Submit** button

Once you click on Submit button, you shall receive your 'User Name' on your registered mobile number.

7.2 Update Mobile Number

In case, you want to update your registered mobile number, click on "**Update Mobile Number**" after logging

I. Enter your new mobile number in "**New Mobile Number**" field (Mandatory)
II. Enter the OTP received in updated mobile number.
III. Type security answer for authentication

IV. Click **Submit** button

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

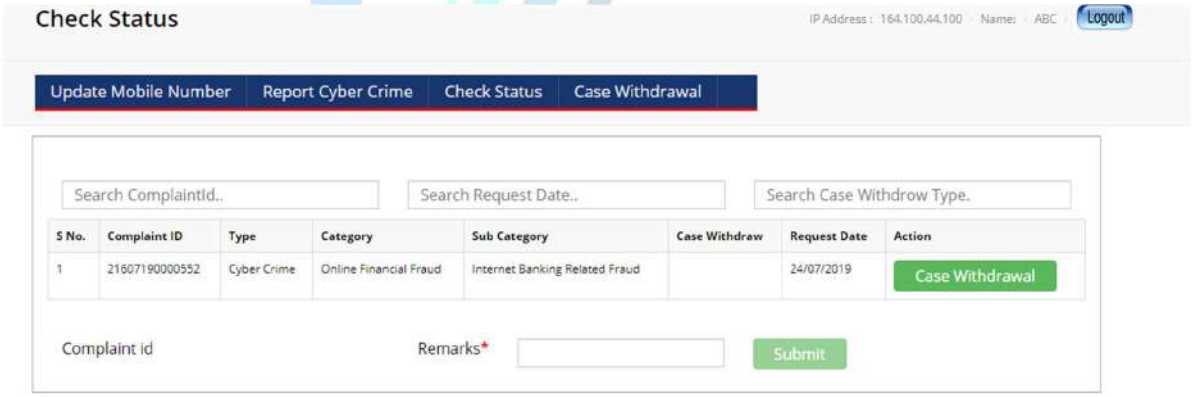
7.3 Case Withdrawal

In case, you want to withdrawal your registered case, click on "**Case Withdrawal**" after logging

I. Select the complaint ID and provide remarks for your complaint withdrawal (Mandatory)

II. Once you click on "submit" your case shall be withdrawn successfully.

Note: You shall not be able to withdraw a complaint, if FIR has been lodged.



Annexure A: Types of various cybercrimes which can be reported by the citizens

S.NO.	CATEGORY	SUB-CATEGORY
1	CHILD PORNOGRAPHY (CP)/CHILD SEXUAL ABUSE MATERIAL (CSAM)	Not Applicable
2	RAPE/GANG RAPE(RGR)-SEXUALLY ABUSIVE CONTENT	Not Applicable
3	SEXUALLY EXPLICIT CONTENT	Not Applicable

S.NO.	CATEGORY	SUB-CATEGORY
4	SOCIAL MEDIA RELATED CRIMES	CYBER BULLYING / STALKING /SEXTING FAKE/IMPERSONATING PROFILE PROFILE HACKING IMPERSONATING EMAIL EMAIL HACKING THREATENING EMAIL ONLINE JOB FRAUD ONLINE MATRIMONIAL FRAUD PROVOCATIVE SPEECH E-MAIL PHISHING
5	ONLINE FINANCIAL FRAUD	DEBIT/CREDIT CARD FRAUD INTERNET BANKING RELATED FRAUD BUSINESS FRAUDS/EMAIL TAKEOVER FRAUD CALL/VISHING E-WALLET RELATED FRAUD SIM SWAP FRAUD
6	RANSOMWARE	RANSOMWARE
7	HACKING	UNAUTHORISED ACCESS/DATA BREACH WEBSITE RELATED/ DEFACEMENT
8	CRYPTOCURRENCY RELATED CRIME	CRYPTOCURRENCY RELATED FRAUD
9	ONLINE TRAFFICKING	ONLINE TRAFFICKING
10	ONLINE GAMBLING	ONLINE GAMBLING
11	ANY OTHER CYBER CRIME	OTHER

Annexure B: Help

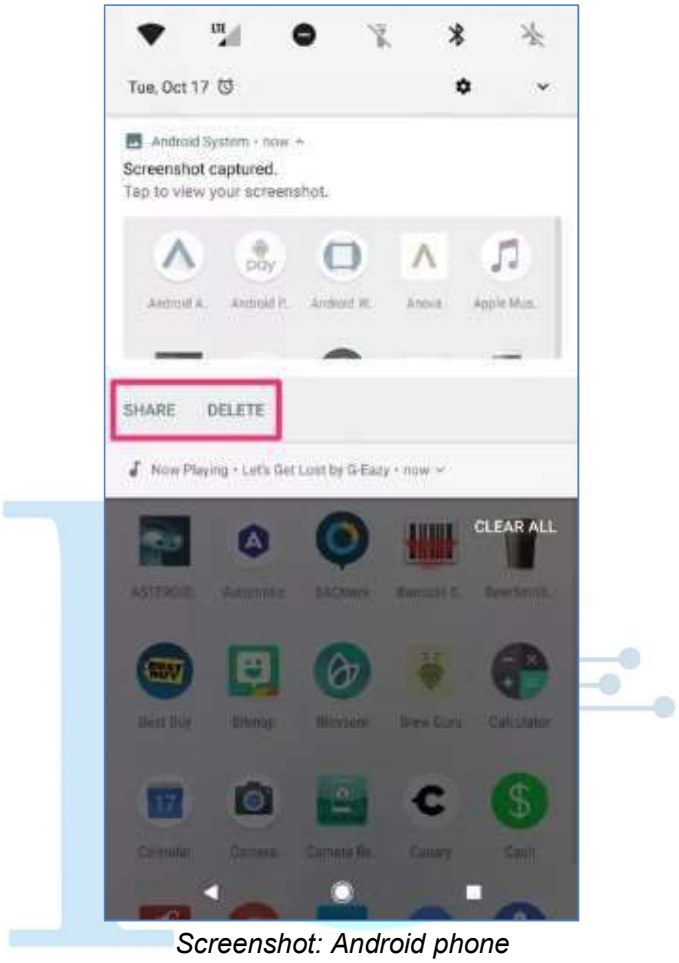
1. How to take a screenshot on Smartphone device

1.1 Android screenshot

Following are the steps to take screenshot from your android smartphone:

I. Navigate to the screen you want to take a picture of.
II. Hold the Power button down for a few seconds.
III. Press “Screenshot” on your phone screen.

IV. If that doesn't work, hold the Power and Volume buttons at the same time for a few seconds.
V. If you see an animation of your screen shrinking, your phone has taken a picture of your screen and saved it in your photos app.
VI. You can find the image in the Screenshots folder under Gallery app.
VII. Attach the screenshot as evidence on attachment.



Screenshot: Android phone

1.2 iPhone screenshot

Following are the steps to take screenshot from your iPhone:

I. Open the app or screen you want to capture.
II. Set up everything exactly the way you want it for the shot.
III. Press and hold the Side button on the right side of iPhone X, iPhone XS, iPhone XS Max, or iPhone XZR.
IV. Click the Volume Up button at the exact same time. (This replaces the Home button step from previous iPhones.)
V. The screen will flash white and you will hear the camera shutter sound (if your sound is enabled).

Screenshot: iPhone

2. How to view and copy Facebook URL/Link:

2.1 From desktop or laptop View

I. Click on the image/video/post whose URL you want to view.

II. The full URL will be seen on the address bar

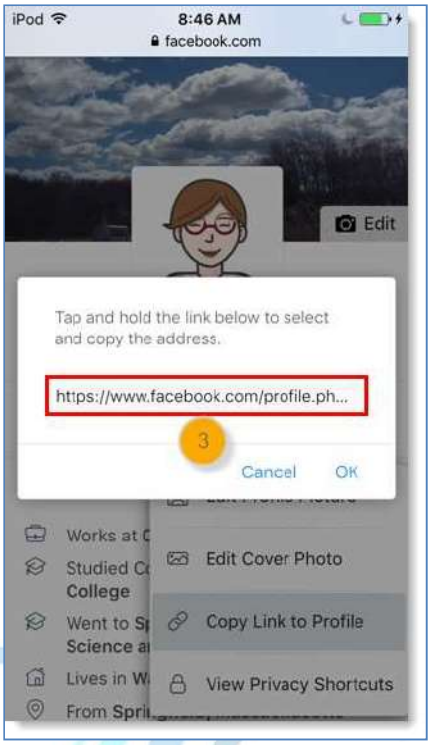
III. Copy the Facebook Profile URL/Page/Post in the address bar of your browser into a file or document. (*Ex: Facebook Profile URL facebook.com/profile.php?id=123456)*

Screenshot: Facebook Profile URL

2.2 From mobile view

I. Open Facebook on your mobile device, navigate to the profile page, and click more.

II. Select “Copy Link to Profile”



Screenshot: How to Copy Facebook User Profile from mobile

III. Click on “Copy the link”.

Screenshot: Facebook Copy Link

IV. To see the URL, you have to paste it on notepad or any text editor

3. How to view and copy YouTube URL/Link:

3.1 From desktop or laptop view

I. Click on the video whose URL you want to view.
II. The full URL will be seen on the address bar
III. Copy the YouTube URL in the address bar of your browser into a file or document

Ex: YouTube URL (youtube.com/watch?v=-qACQjC5J0w)

Screenshot: How to copy YouTube URL

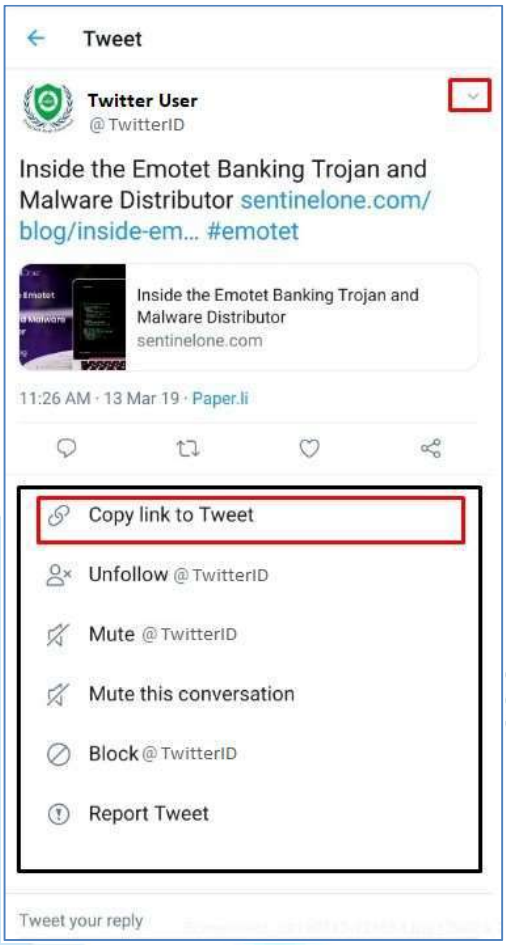
3.2 From mobile view

I. Open the YouTube app on mobile
II. Look or search for the video you want to copy
III. Find the tripe vertical dots on the top right corner of the video thumbnail or details
IV. Tap on it and select “Share”

V. You will see a new Share window, select “**Copy link**”
VI. Simply paste the link it on notepad or any text editor

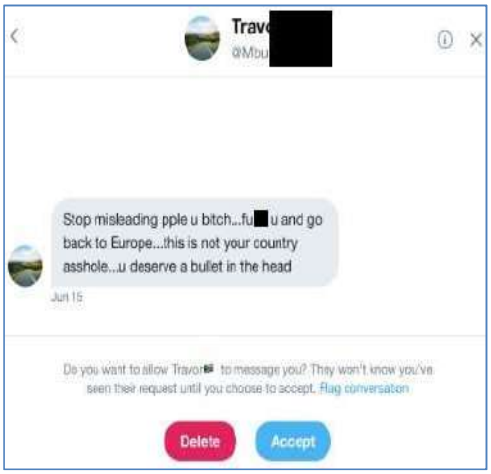
4. How to copy Twitter Post URL

I. Navigate to the Tweet you'd like the URL of.
II. Tap the drop-down arrow
III. Select **Copy link to Tweet**. The URL should now be copied to your clipboard.



Screenshot: Copy twitter tweet link

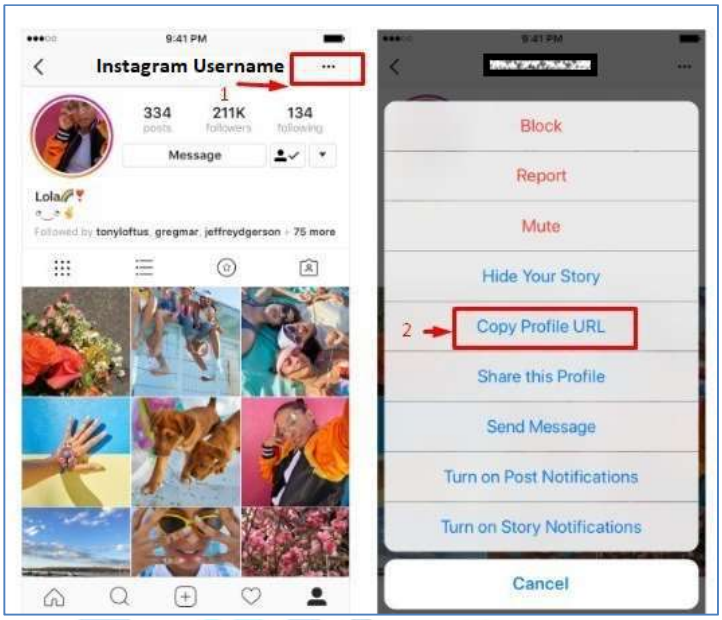
IV. To take a screenshot of twitter message, navigate to the inbox chat message and take screenshot. It will also capture the twitter user ID (@Twitter ID).



Twitter Message Snapshot

5. How to copy Instagram User profile URL

In the Instagram app, find the photo or video you want to copy the URL. When you have found it, tap on the" **…**" icon above it. This will bring up several options. Select **Copy Profile URL** Link



Screenshot: Instagram Profile URL

As well, navigate to the Instagram message inbox and take a screenshot of the chat

Screenshot: Instagram Chat/User Profile

6. How to export WhatsApp chat

Following are the steps for WhatsApp Application chat

6.1 WhatsApp chat screenshot

I. Navigate to the chat screen for the individual or group you want to take a picture of. (Provide the name and number of the sender/group)

II. You can find the image in the Screenshots folder under Gallery app.

WhatsApp IM Chat screenshot

6.2 Export Chat from Android

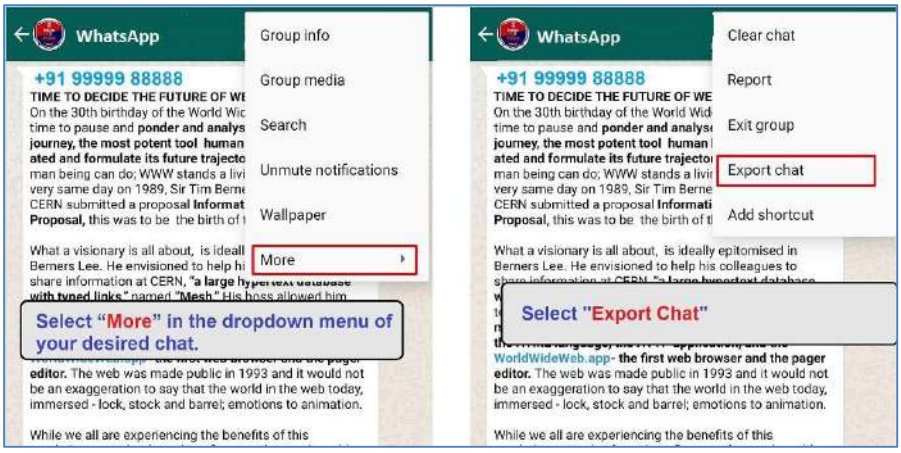
To export a copy of the history of an individual chat or group, use the Export chat feature:

I. Navigate to the chat screen for the individual or group you want to take a picture of.

II. Tap More options ⋮ .

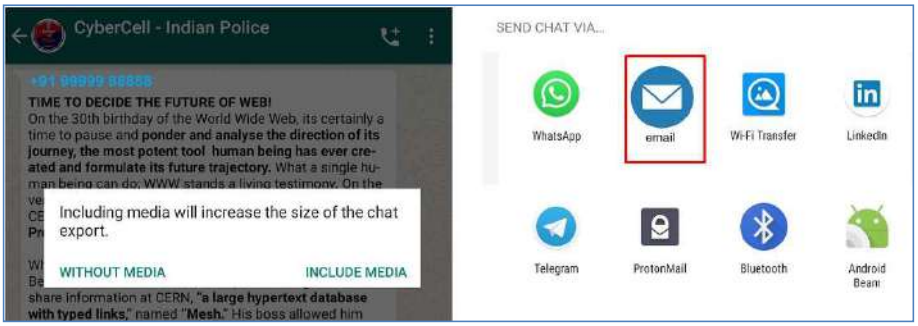
III. Tap More.

IV. Tap Export chat.



Screenshot: Export WhatsApp Chat

Choose whether to Include Media or not.



Screenshot: Export WhatsApp chat on Mail

An email will be composed with your chat history attached as a .txt document.

Note:

- If you choose to attach media, the most recent media sent will be added as attachments.
- When sending with media, you can send up to 10,000 latest messages. Without media, you can send 40,000 messages. These constraints are due to maximum email sizes.

6.3 Export chat from iPhone

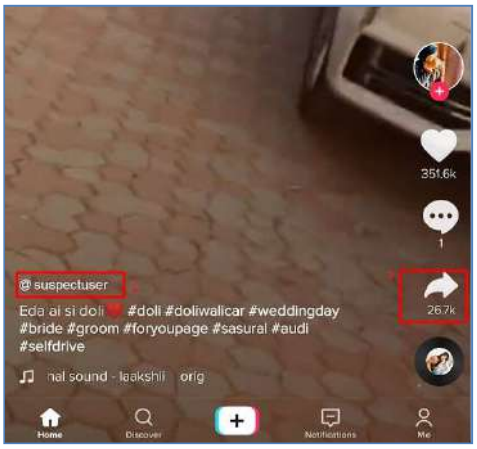
You can email yourself a chat history if you'd like to save a chat:

I. Open the WhatsApp chat you want to email.
II. Tap the contact's name or group subject.
III. Tap Export Chat.
IV. Select if you want to Attach Media or email the chat Without Media.
V. Tap the Mail app. You can also tap More for additional options.
VI. Enter your email address and tap Send.

7. How to copy TikTok video URL

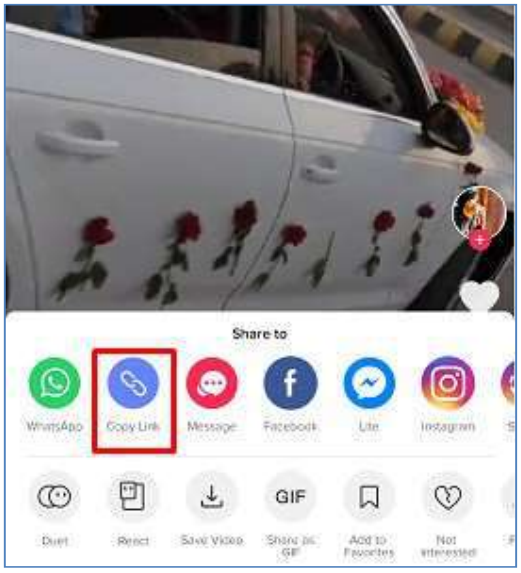
TikTok app is a social media platform for creating, sharing and discovering short music videos, think Karaoke for the digital age. Following are the steps to copy TikTok profile or social media post using a smartphone

I. Open TikTok on your phone; Open the video and take a screenshot as well copy of the suspect TikTok userID. Ex.@suspectuser



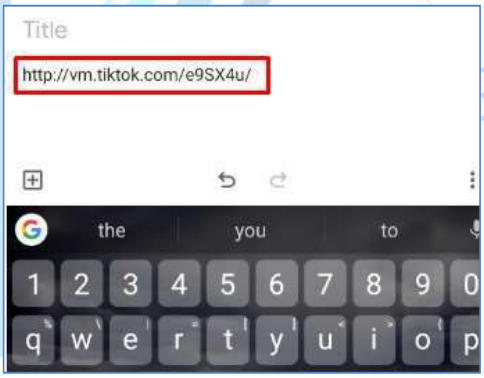
Screenshot: TikTok User ID

II. You can copy the video link by clicking on share link option, after that it will open new windows via any email, messaging, or social media app in the list. This opens a new message or post in the selected app.



Screenshot: Copy Link of Tiktok Video

III. Click on the Copy link and paste it on any file or document.



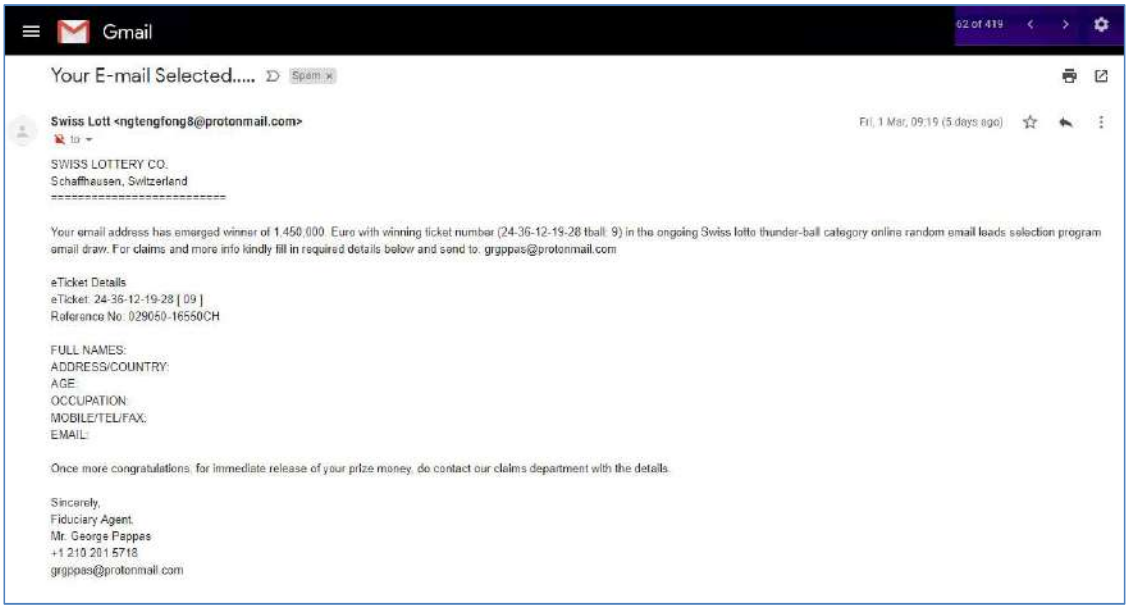
Screenshot: Example of TikTok Video URL

8. How to export and copy E-mail Header

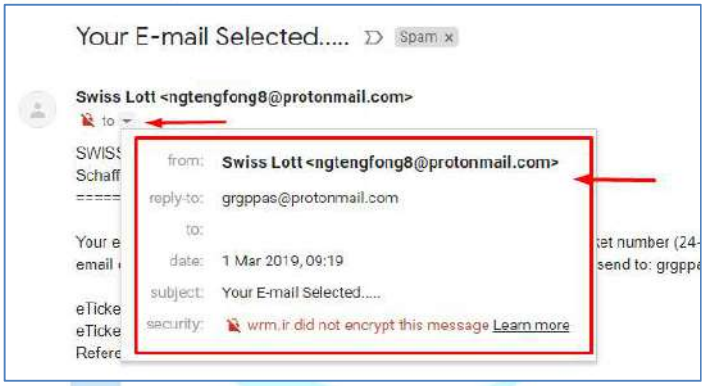
Following are the steps for how to copy and save email headers:

8.1 Gmail email header

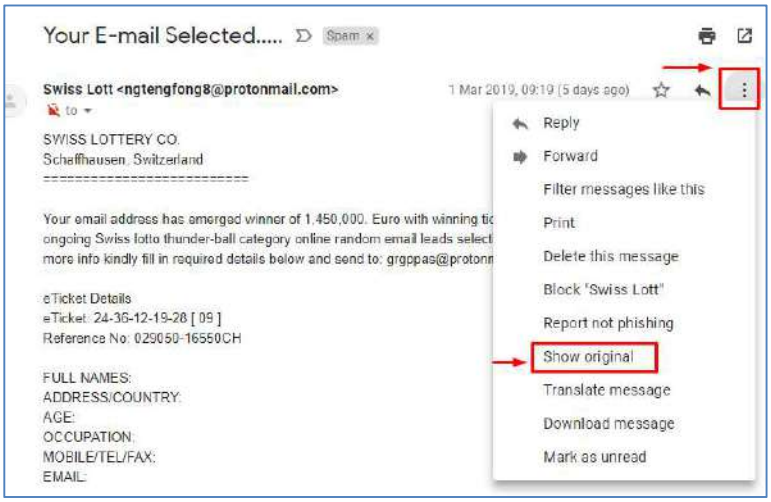
I. To get an email header from Gmail, open the email within your web browser.



Click on drop-down arrow and see the senders & reply-to email

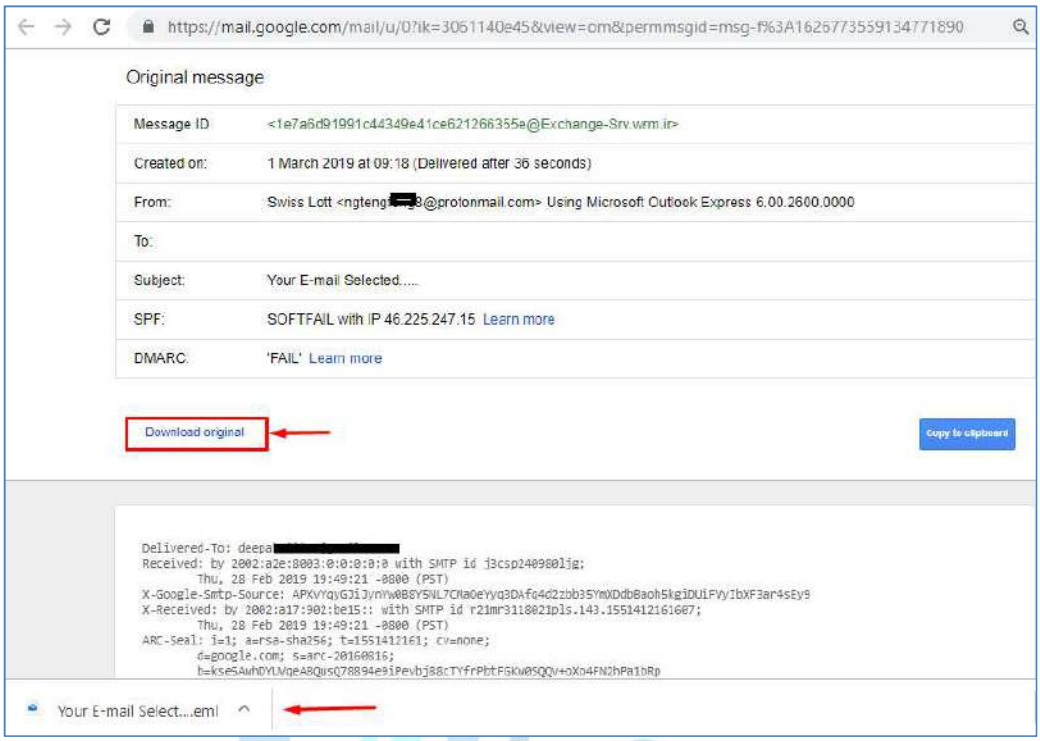


Click the drop-down arrow (more) next to the reply button and choose "**Show Original**".



Once the new page opens then click on "**Copy to Clipboard**" then paste the copied content in notepad or any text editor.

Otherwise you can download the email by clicking on “Download Original”, all email content including header will get download as **.eml** format. Attach this (.eml) downloaded file as evidence.

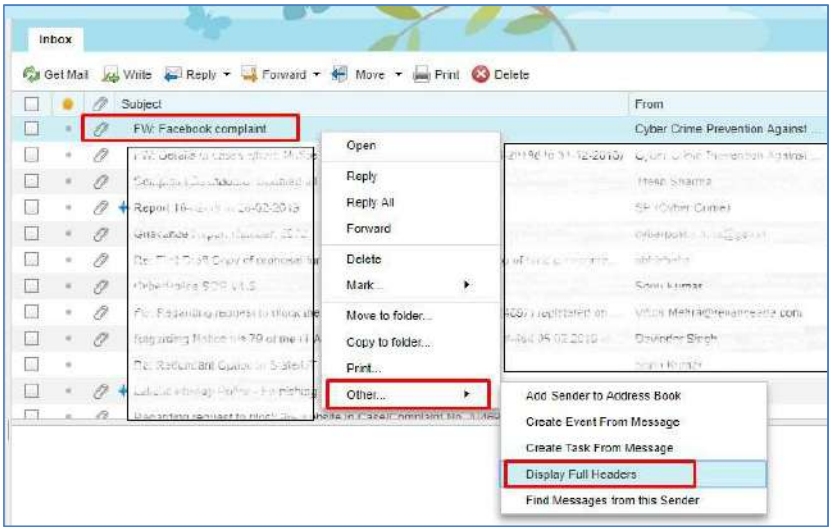


Download Email in (.eml) format

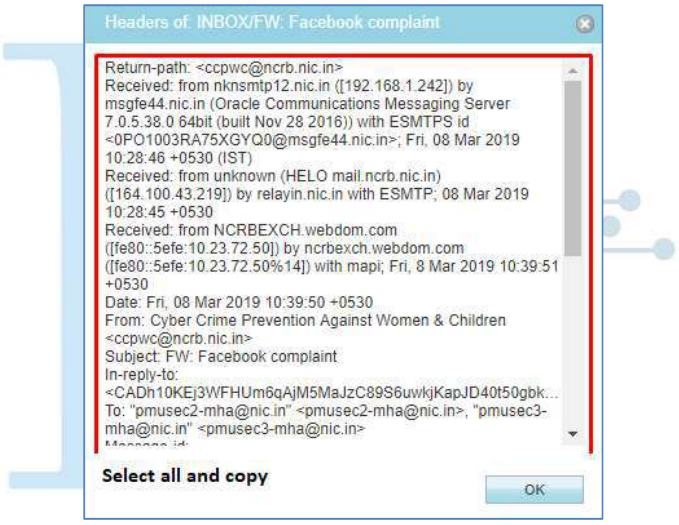
8.2 NIC mail Header

Following are the steps to copy email header of NIC mails

I. Open the NIC email within your web browser.
II. Right click on mail and navigate to **Other→Display Full Headers**



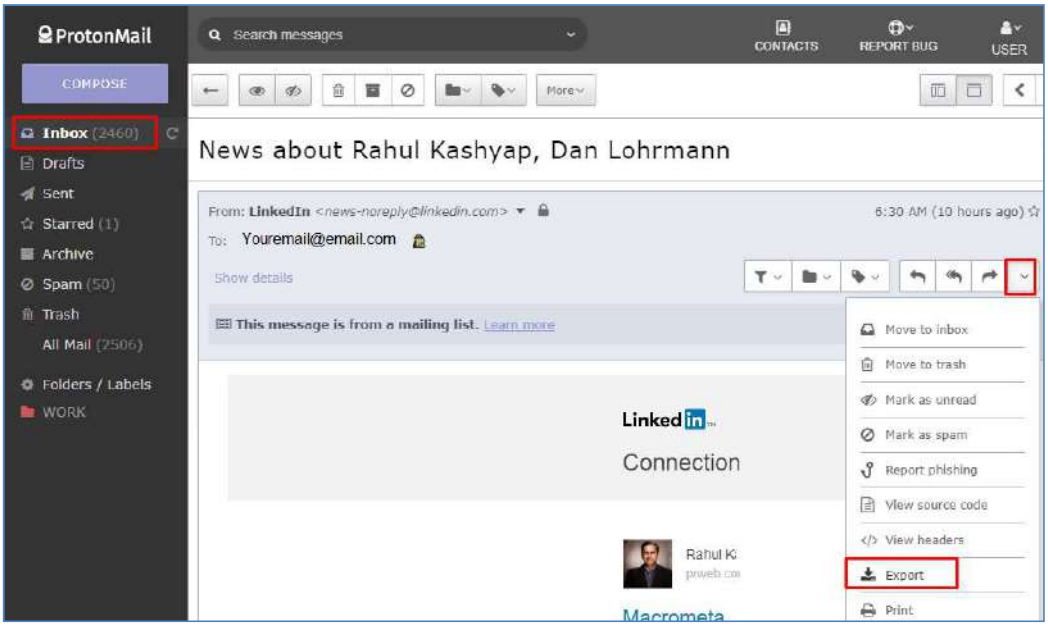
III. After clicking on **Display Full Headers**, a pop-up window will appear. Then scroll down and copy all email headers; paste on notepad or any document.



8.3 ProtonMail email Header

Following are the steps to export ProtonMail email headers in (.eml) format

I. Open the email within your web browser.
II. Click on drop-down arrow and see the senders & reply-to email
III. Click the drop-down arrow (more) next to the reply button and choose "Export".



After click on “Export”, email header data will download as **.eml** format then send as attachment.

For Yahoo Mail Header following are the steps:

I. Log in to Yahoo! Mail.
II. Open the message for which you wish to view the headers.
III. Click the More (gear) icon above the message pane.
IV. In the menu, select View Raw Message. A new tab opens containing your message’s headers, which you can now copy and paste.

For Outlook Mail Header following are the steps:

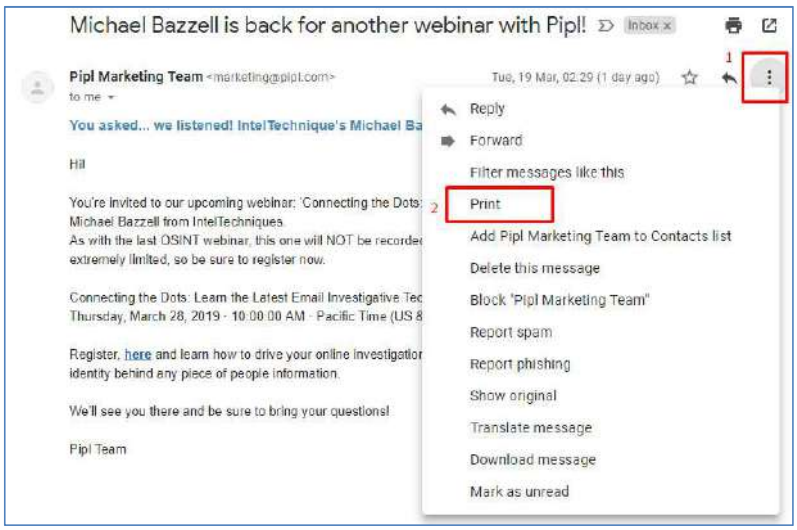
I. Login into your account
II. Select Inbox from the left-side menu
III. Open the message you want to see the header and click file tab
IV. The full headers will appear in a new window.

For other mail refer to https://mxtoolbox.com/public/content/emailheaders/

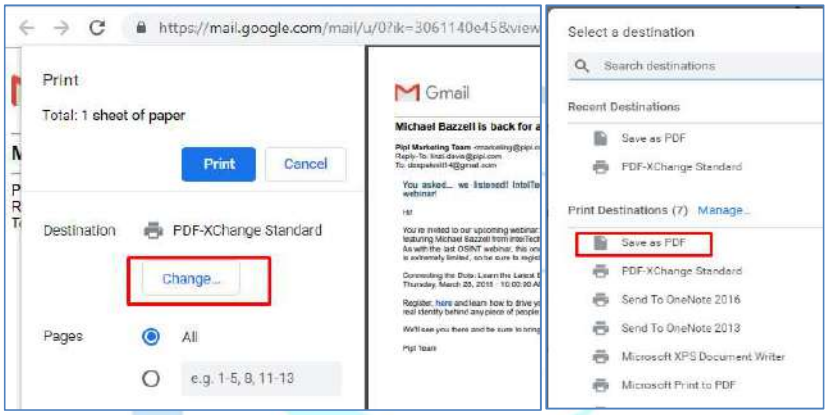
8.4 How to save email in PDF

8.4.1 To save Gmail email in pdf

I. To save a Gmail email in PDF format, open the email within your web browser.
II. Click the drop-down arrow (more) next to the reply button and choose "**Print**". Or Click the printer icon. It’s near the top-right corner of the message.
III. Click “**Print**”. The Gmail Print screen will appear.

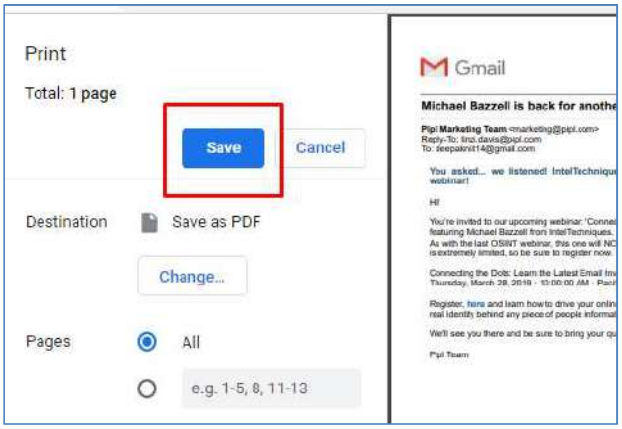


IV. Click **Change**. It's beneath the printer in the left column of the print screen. Click Save as "**PDF**"

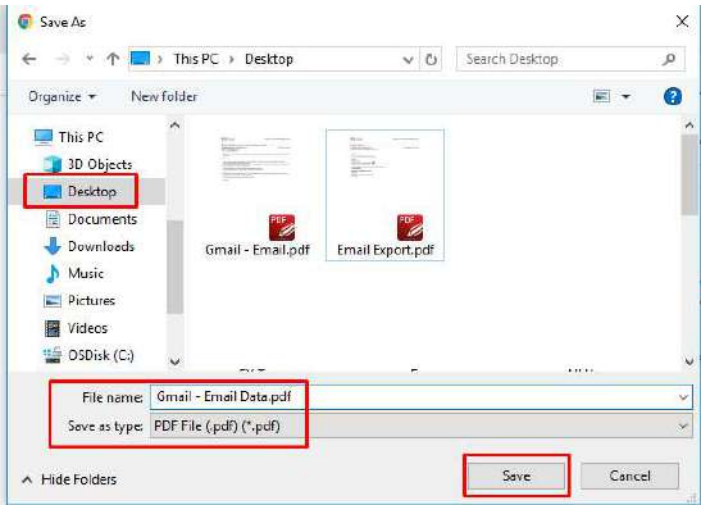


Screenshot: Save as PDF

V. Click Save. The email message will now download to your computer as a PDF file.



Screenshot: Click on save



Screenshot: Save Email as PDF

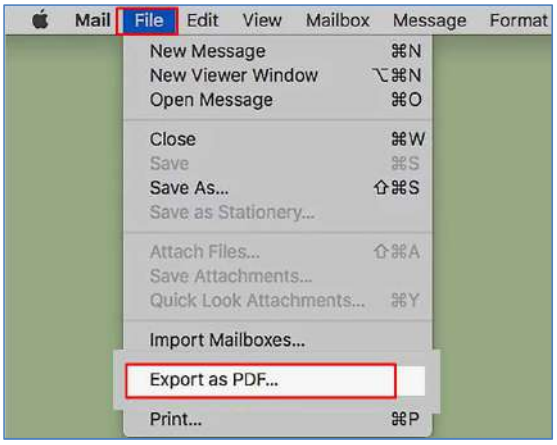
8.4.2 Using the Mail App on a Mac

I. Open the Mail app. It's the icon of a stamp with an eagle inside. You'll usually find it on the Dock and on the Launchpad.

Screenshot: Open Mail App

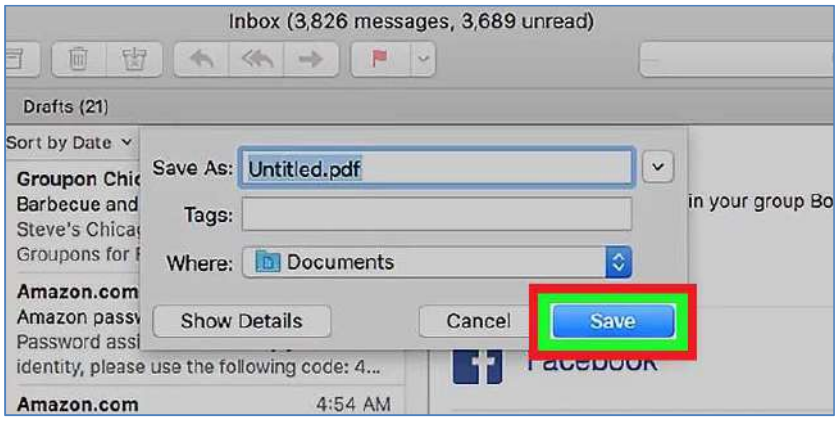
II. Click the message you want to download as a PDF.

III. Click the File menu. It's in the menu bar near the top-left corner of the screen.



Screenshot: Export mail as PDF

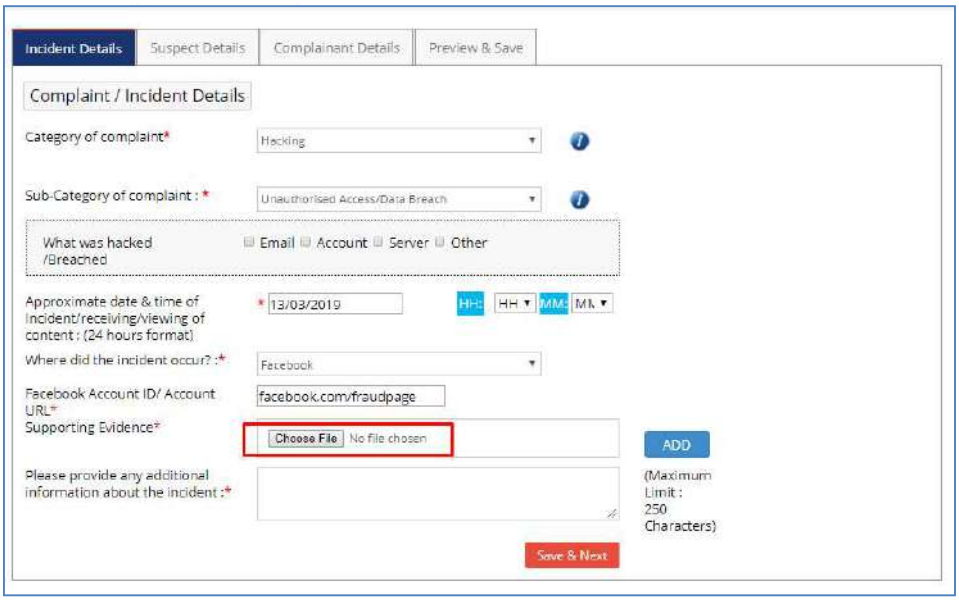
IV. Click Export as PDF. Select a saving location.
V. Click Save. The PDF is now saved to the selected folder.



Screenshot: Save Mail in PDF

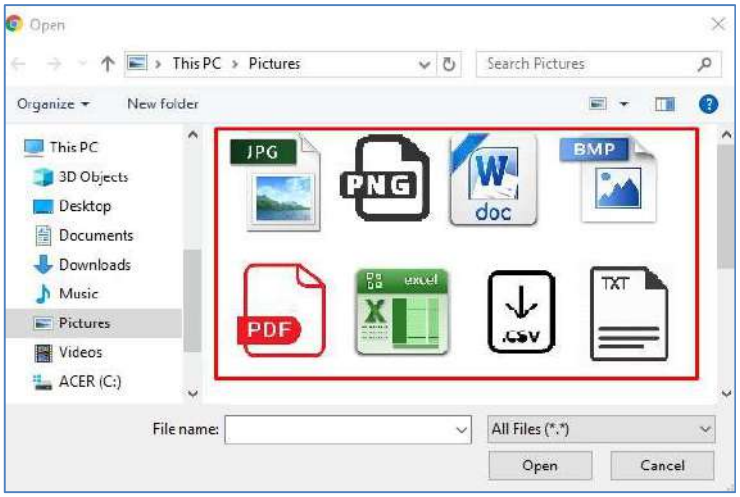
9. How to upload any evidence on the portal

Navigate to Supporting option under Incident Details, click on “Choose File”.

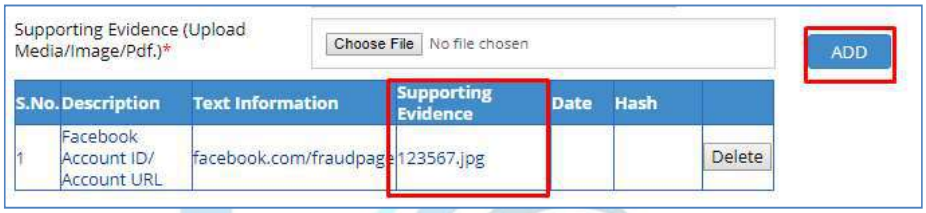


Screenshot: Upload evidence

Note: Select the evidence for the attachment. This upload feature accepts .txt .png .jpeg. jiff .rtf .jpg .dib .gif .doc .ppt .docx .pptx .pdf. epub .bmp .avi .wmv .3gp .mp4 .mkv .mov .flv .mpg. webm file types and the maximum file size of 5 mb.



After selecting the evidence then click on **Add** button.



Annexure C: Sample of Evidences

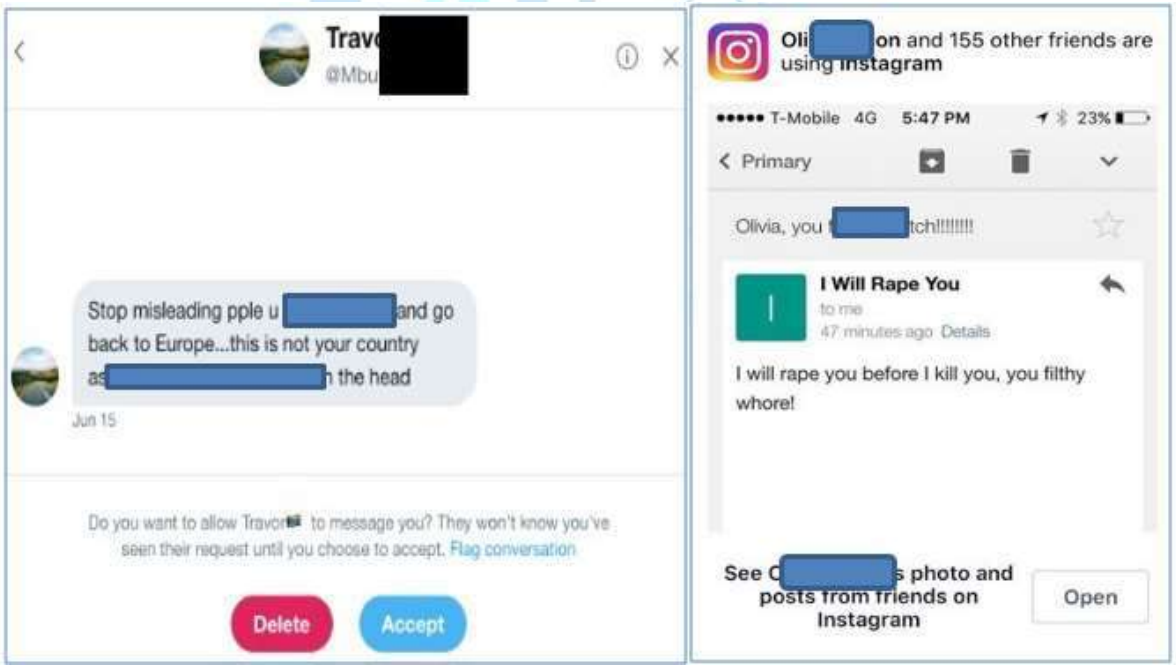
To report a complaint user shall have following evidence/information details may include, but not limited to:

- Copy or screenshot/s of alleged contents/profile
- Screenshot copy of URL of alleged contents
- Alleged and user Email ID, Contact details
- Bank statement from the concerned bank
- Take a copy or screenshot/s of SMSs received related to the alleged transactions
- Copy of your ID proof and address proof as shown in the bank records
- Contents should be in both hard & soft forms
- Email should be taken from the original receiver. Copy of the forwarded email should be avoided
- Full Header of the alleged Email (prefer .eml format)
- Copy of email and header should be in both hard & soft forms

Following are some evidence samples which may be provided on the other online cybercrime categories:

3.1 Sample Evidence for Cyber Cullying/Stalking/Sexting

Following are some evidence samples which may be provided on the Cyber Cullying/Stalking/Sexting categories



Screenshot: Twitter & Instagram Chat/User Profile

3.2 Sample Evidence for Fake Impersonating Profile

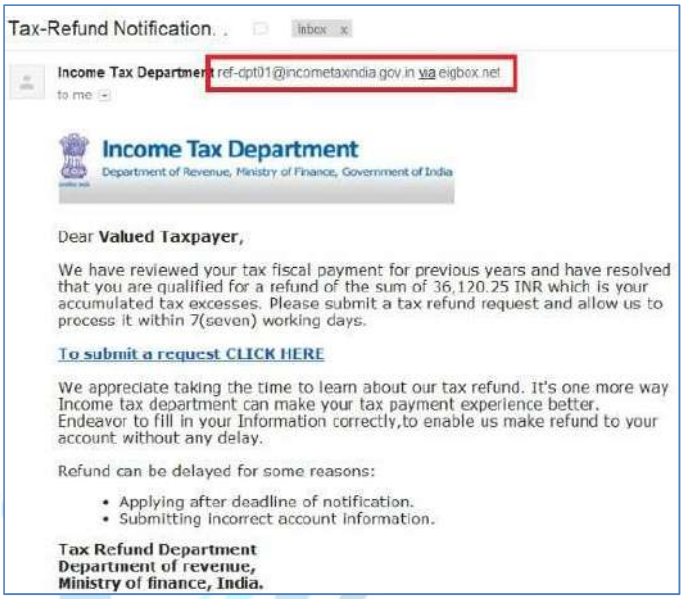
Following are some evidence samples which may be provided on the Fake impersonating profile categories

*(For example, attached fake Twitter ID: @wc**********n_)*

3.3 Sample Evidence for Impersonating Email

Following are some evidence samples which may be provided on the impersonating email category:

Suspect Email ID: ref-dpt01@incometaxindia.in



Screenshot: Impersonating mail

3.4 Sample Evidence for Online Job Fraud

Following are some evidence samples which may be provided on the online job fraud category:

For example, need to provide details on portal:

Person Name : Mr. Shashank
Company : Airways LTD
Address : Jet Limited, 319, Udyog Nagar Vihar, Phase IV, Gurgaon -122016
Email : career@job.com, number: +91-99999-88888

Airways LTD

Airways LTD
ADDRESS :- jet Limited, 319,
Udyog Nagar Vihar, Phase IV,
Gurgaon - 122016

We are informing you that your resume has been online selected in our annual direct selection of candidates through our direct interview in AIRWAYS LTD.

Your code number – SJL- 011. You are in group One.
The Company offers you to join as an post in respective department. You are selected according to your resume in which Project you have worked and on the basis of your academic records.

DEPARTMENTS: – GROUND STAFF & CABIN CREW EXECUTIVES & MANGER'S, HR & Administration, Accountants & Finance Executive, Cashier, Chartered Accountant, Company Secretary, Back Office, Purchase & Store, Legal Advisor, Aeronautical Engineer, Radio Engineer, Technical Support Engineer, Aircraft & Aviation Technician (Engineers), Electrical Engineer, Line Maintenance, Fire & Safety And Security, Medical Officers, IT Hardware & Networking, Software Engineers, Customer Support Executive, BPO Etc & Other According to Your Resume.

TOTAL - 95 candidates Short-Listed, Post - 75, Experience: 0 to 10 Years
JOB LOCATIONS: - New Delhi, Uttar Pradesh, Andhra Pradesh, Tamil Nadu, Gujarat, Rajasthan, Maharashtra, Punjab & Others.
INTERVIEW DATES: - **28th September 2016** at Corporate Head Office, GURGAON.

The Selected candidate keeps the right of being getting posted at the desired location subject to the final decision of HRD after discussion. Salary - Min –Rs.35, 000/- to Rs.120, 000/-per month + incentives, per month on your performance .You are going to get employment in Airways LTD

NOTE - You have to deposit an refundable security amount by Cash Rs 9950 /- Rs 07/09/2016 into The Bank **(UNION BANK, VIJAYA BANK & CENTRAL BANK)** The Job profile and salary offered by Company will be mention in your call latter. Your call latter and Air Ticket will dispatch very shortly after receiving your confirmation of security deposited in to the Bank. The security amount paid by the candidate is refundable amount.

NOTE - 07/09/2016 is the last date of security deposit in to the bank for A/C Number you can Make a call **MR. SHASHANK** . 9:00 AM to 6:00 PM.
Late reporting candidates will be not allowed in the process. We are strictly concerned on time management as per the values of the company. The selected candidate visit to company office is not allowed before interview date. Only one family person is allowed with female candidate. This call letter and group code number SJL- 011. Is not-transferable. This code is valid only for your interview date.

1 Note - You come with your all documents photocopy. And one hard copy of the invitation mail. Id Proof, 5 Photos.
2 Note - You can call in official working Hours Monday to Saturday– 9Am to 4 Pm. After the working hours your call will not be accepted.

If you are been selected or not, This amount will be refundable, it is just a security deposit as assuring your presence on the interview date and venue, we will be reserving your air tickets fare upon our expenses, that would be paid by the company itself,

NOTE- After Depositing The Security Deposit, Kindly Send Your Deposit Slip, Photo, Id Proof, Scan Copy, And Your Mobile Number By Mail At Career@job.com

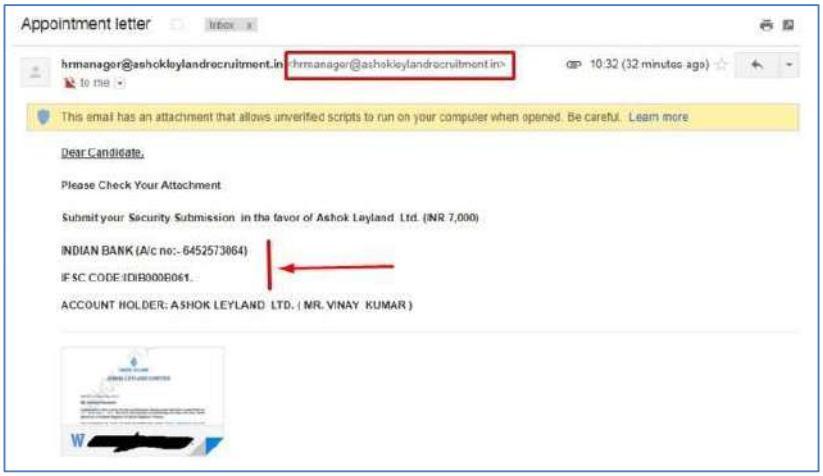
Kindly Give The Information After The Deposit Of The Security Amount In To The Bank To Company's Mentioned Email Id. Without Information Your Letter Will Not Be Dispatch To Your Home Address.

Regards
(Senior Manager)

With best wishes,
Mr. Shashank
+91-99999-88888

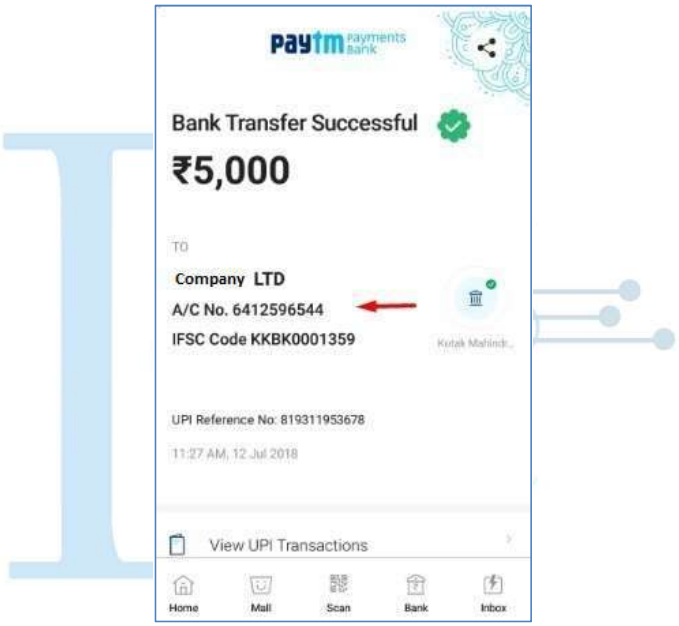
Signature (Manager HR)

Screenshot: Fake Job OfferLetter



Screenshot: Fake Email of HR hrmanager@ashokleylandrecruitment.in

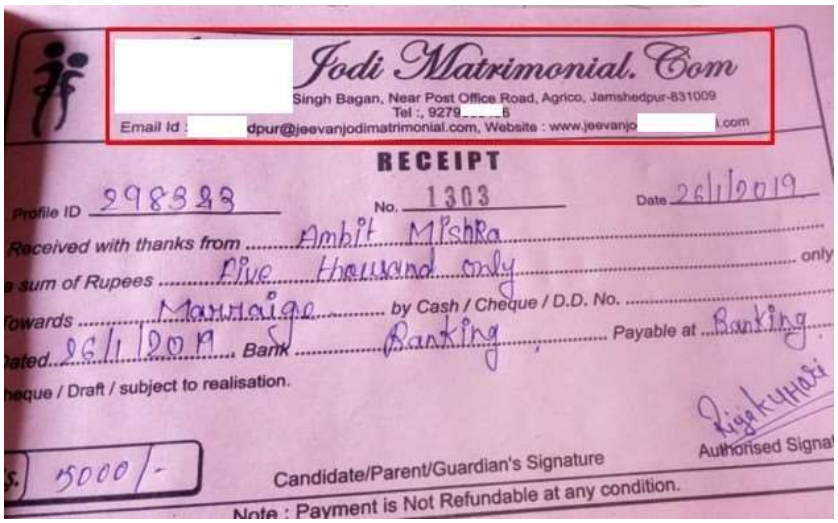
For example: Account details alleged in case: 6412596544



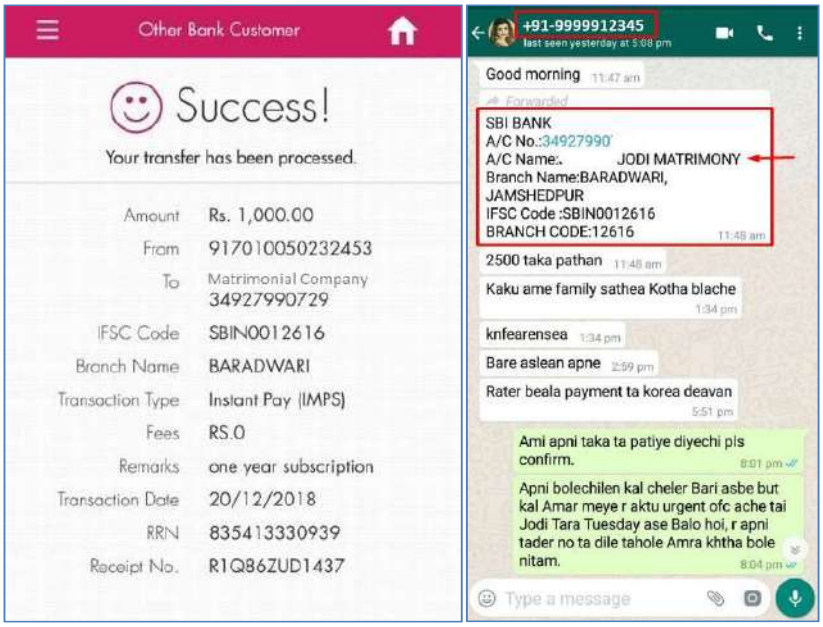
Screenshot: Account Details

3.5 Sample Evidence for Online Matrimonial Fraud

Following are some evidence samples which may be provided on the online matrimonial fraud category:



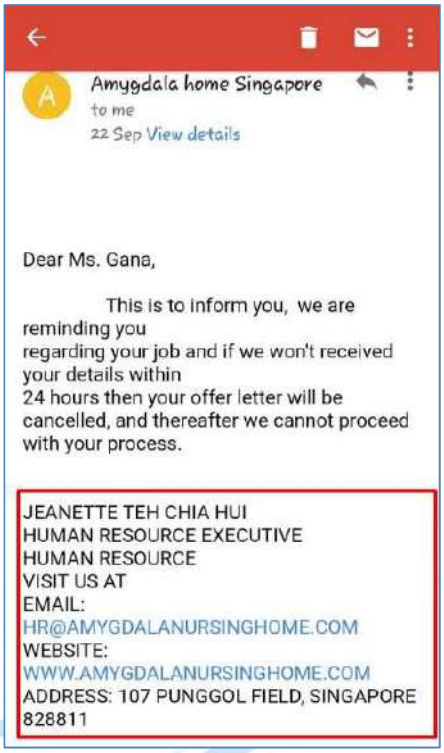
Screenshot: Matrimonial company payment receipt



Screenshot: WhatsApp and Bank transaction details

3.6 Sample Evidence for Threatening Email

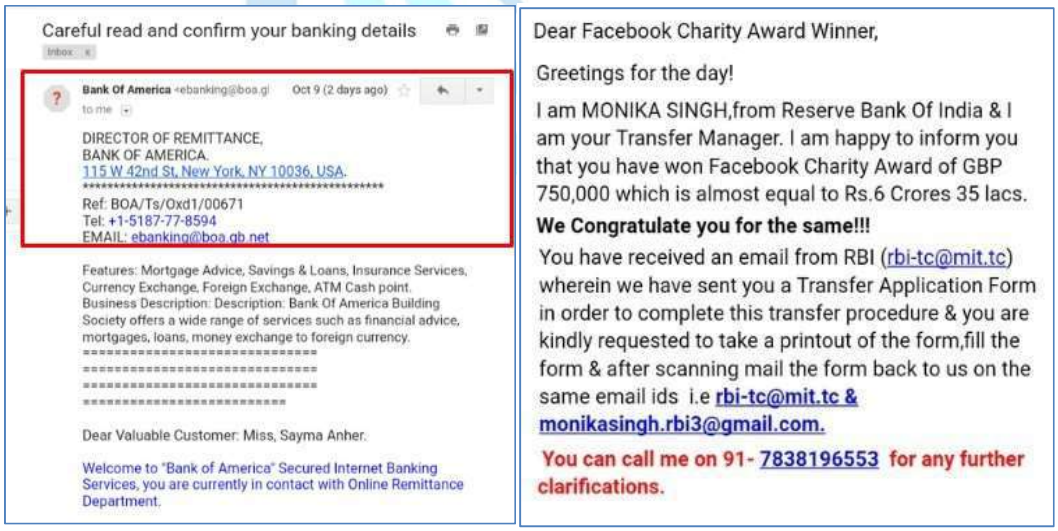
Following are some evidence samples which may be provided on the threatening email category:



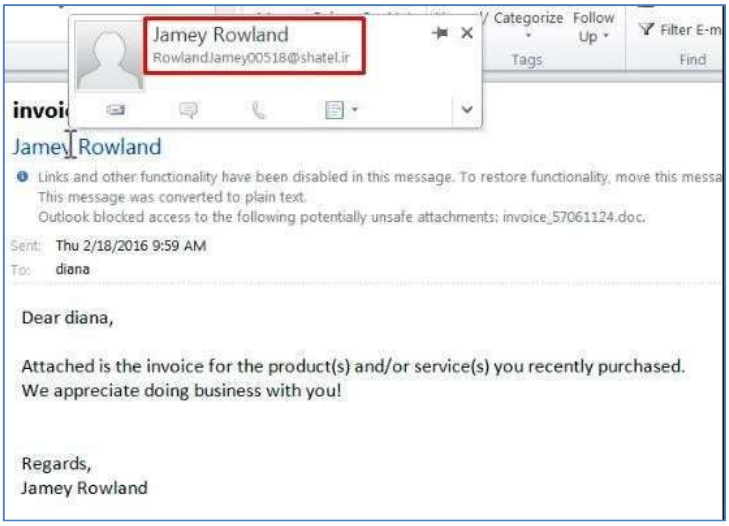
Screenshot: Threatening Email

3.7 Sample Evidence for Business Frauds/Email Takeover

Following are some evidence samples which may be provided on the business frauds/email category:



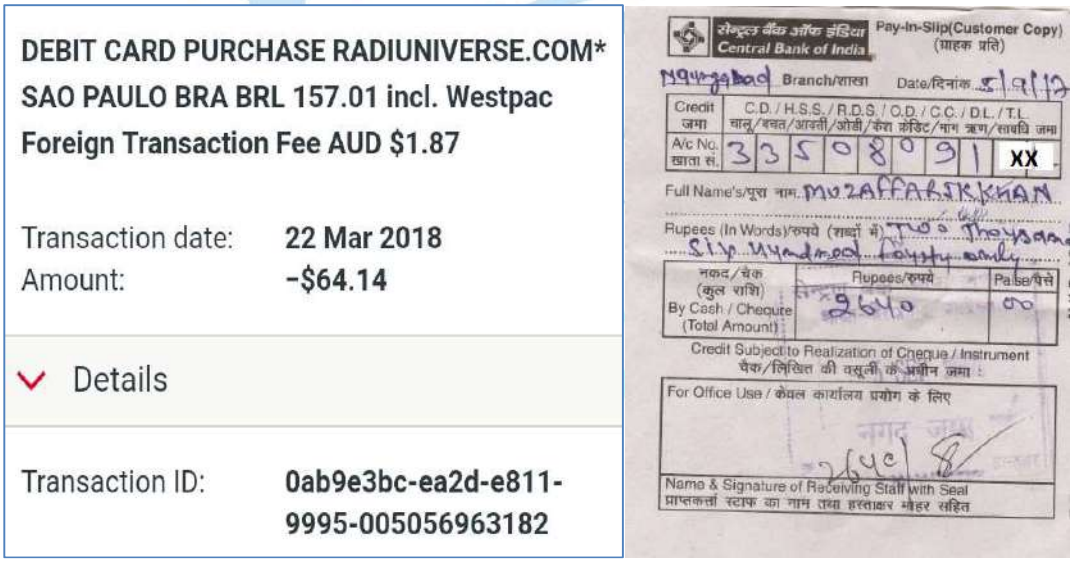
Screenshot: Email Body



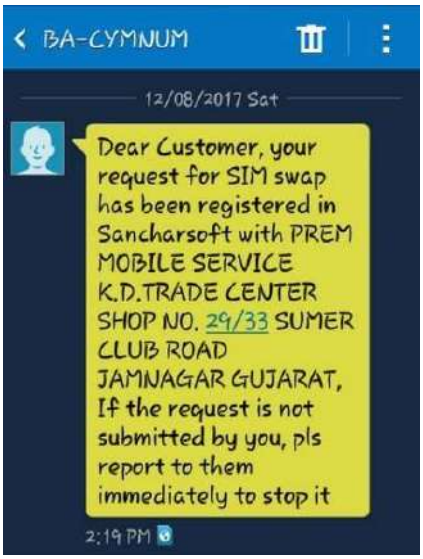
Screenshot: Senders Email

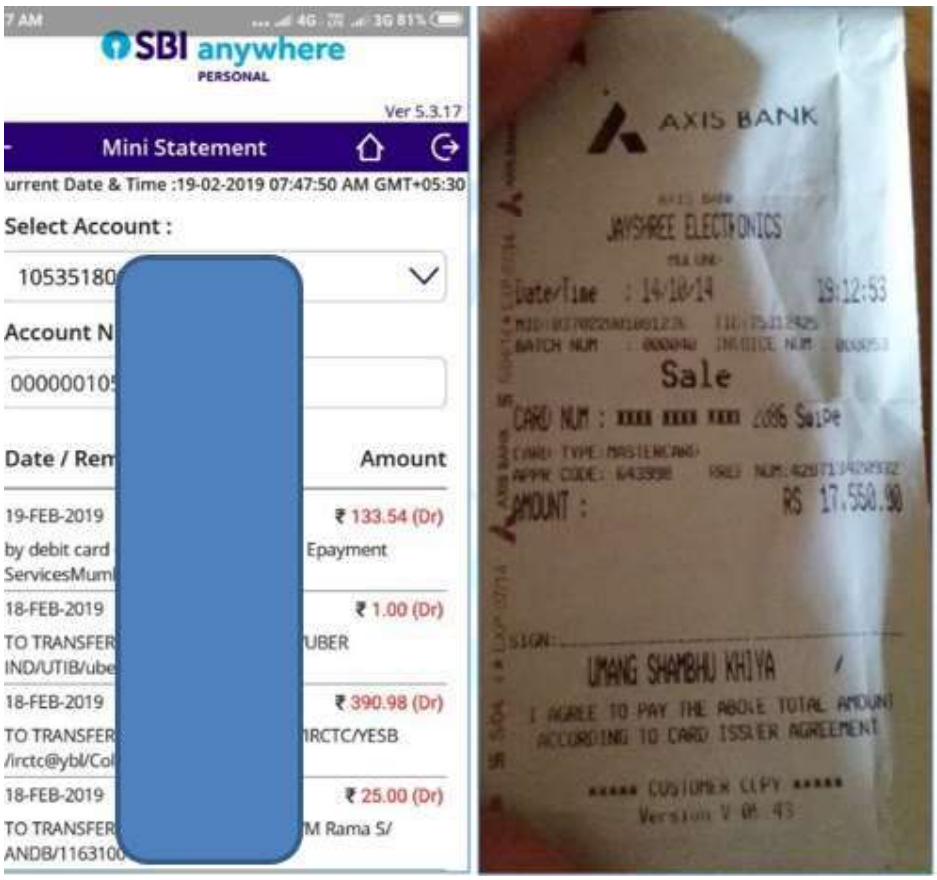
3.8 Sample Evidence for Debit/Credit Card SIM Swap Fraud

Following are some evidence samples which may be provided on the debit/credit card, SIM swap fraud category:



Screenshot: Transaction detail, bank account slip





Screenshot: Mini statement

Screenshot: Notification bank SMS

BULDHANA
BULDHANA 443201
MAHARASHTRA INDIA

JOINT HOLDERS :

Nomination : Not Registered

Currency : INR
Email : Useremail@GMAIL.COM
Cust ID
Account No
A/C Open Date
Account Status
RTGS/NEFT IFSC
Branch Code

From : 04/09/2017 To : 04/09/2017

Statement of account

Date	Narration	Chq./Ref.No.	Value Dt	Withdrawal Amt.	Deposit Amt.	Closing Balance
04/09/17	POS 532676XXXXXX5971 PAYZAPP BILL PAY PO S DEBIT	0000000000974276	04/09/17	10.00		15,968.30
04/09/17	NWD-532676XXXXXX5971-01716030-AURANGABAD	0000724720022842	04/09/17	1,000.00		14,968.30
04/09/17	POS 532676XXXXXX5971 CPONEASSIS POS DEBI T	0000J15635492515	04/09/17	1,899.00		13,069.30

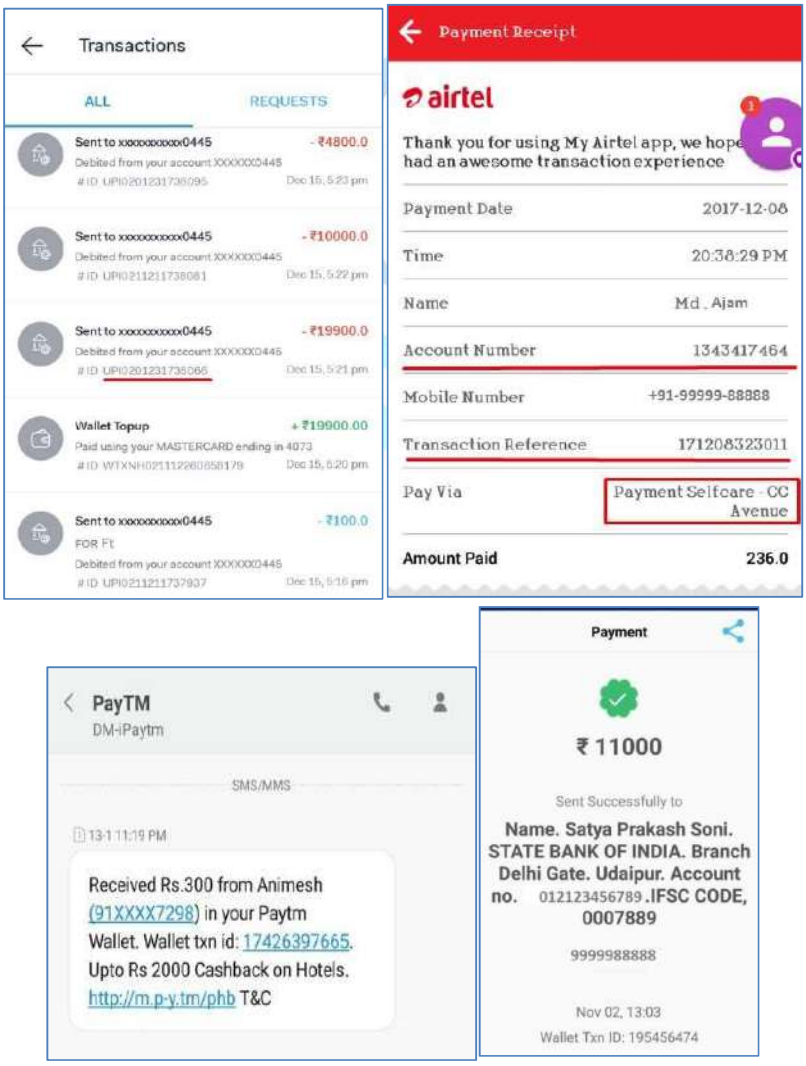
STATEMENT SUMMARY :-

Opening Balance	Dr Count	Cr Count	Debits	Credits	Closing Bal
15,978.30	3	0	2,909.00	0.00	13,069.30

Screenshot: Debit/Credit SIM swap fraud

3.9 Sample Evidence for E-wallet Fraud

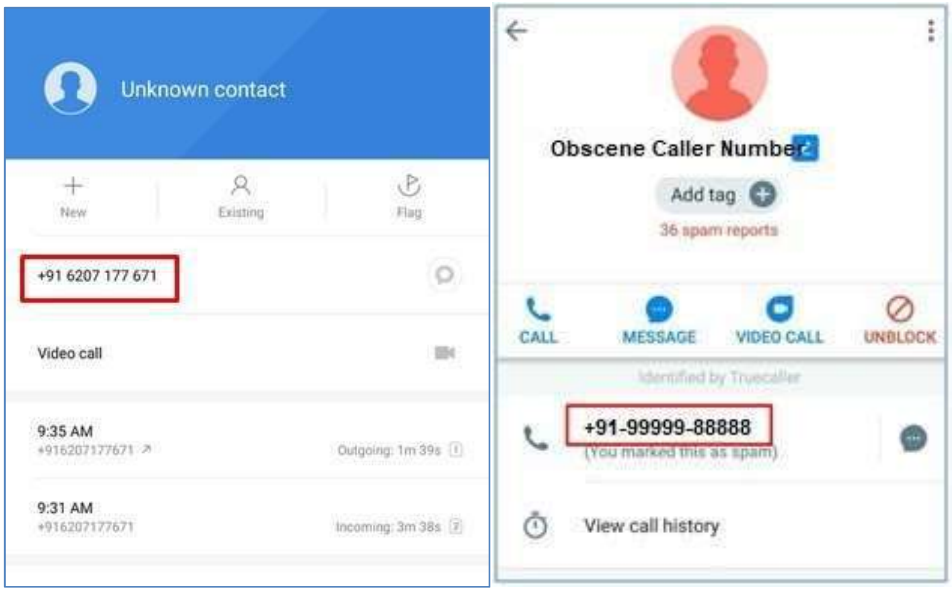
Following are some evidence samples which may be provided on the e-wallet category:



Screenshot: E-wallet transaction frauds SMS

3.10 Sample Evidence for Fraud Call/ Vishing

Following are some evidence samples which may be provided on the fraud call/Vishing category:

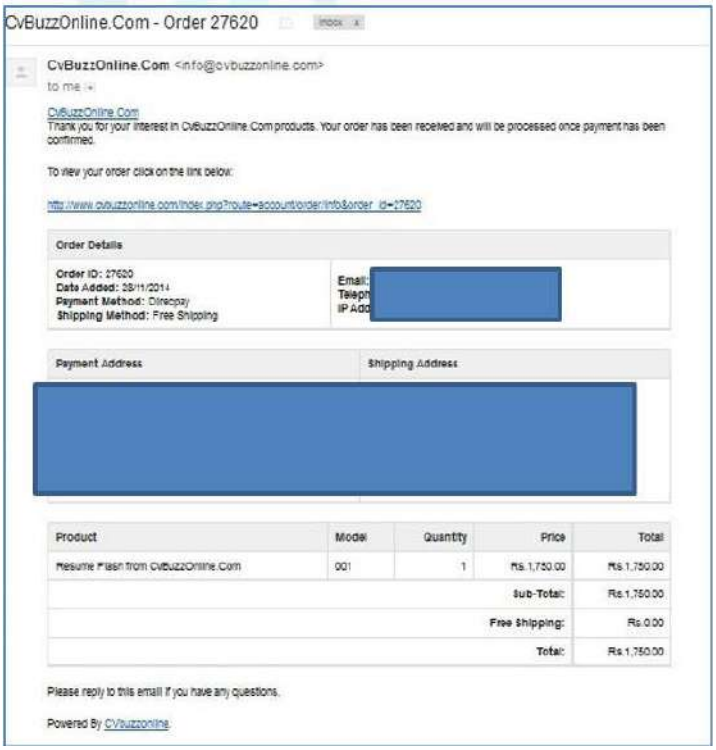


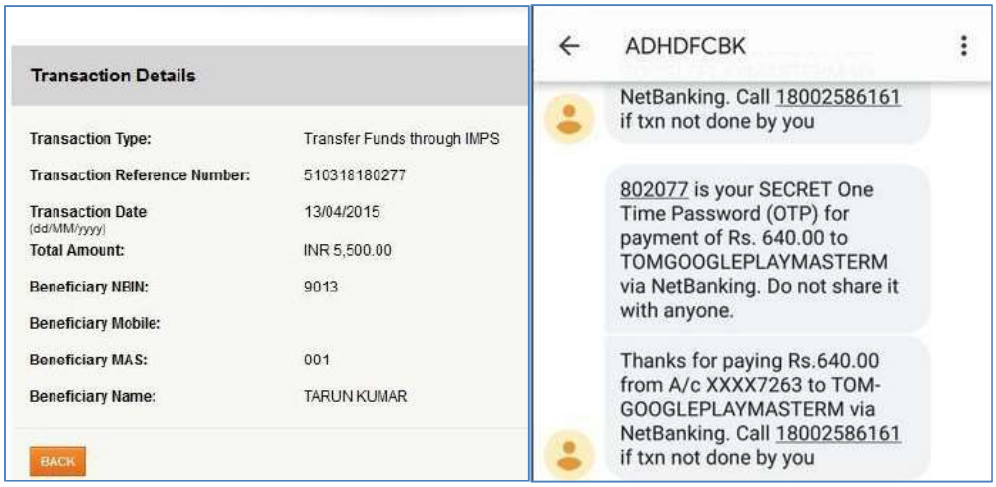
Screenshot: Obscene Caller Number

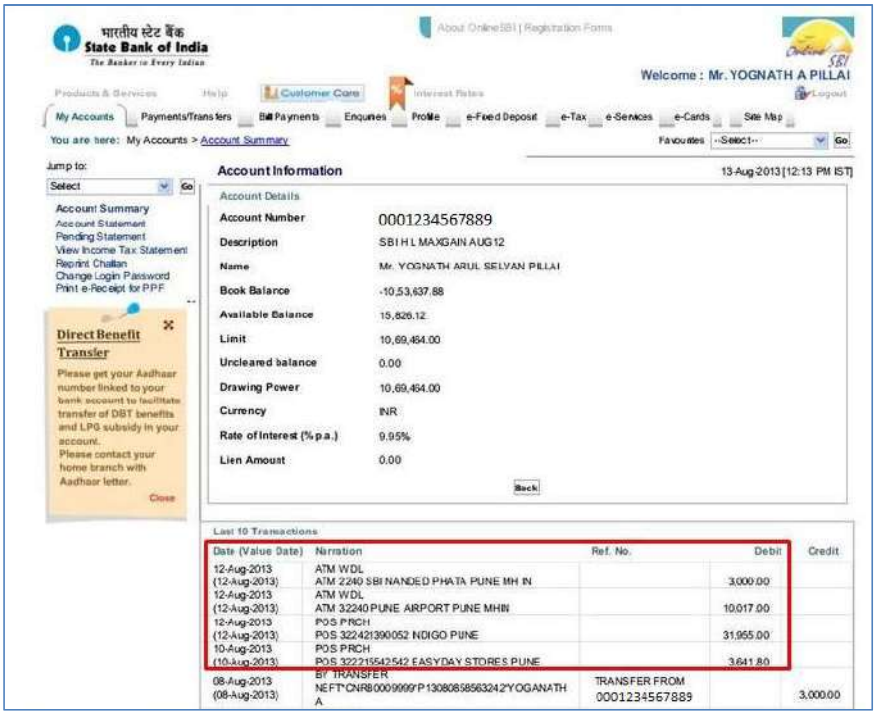
3.11 Sample Evidence for Internet Banking Related Fraud

Following are some evidence samples which may be provided on the internet banking related category:

To report Copy of your ID proof and address proof as shown in the bank records.



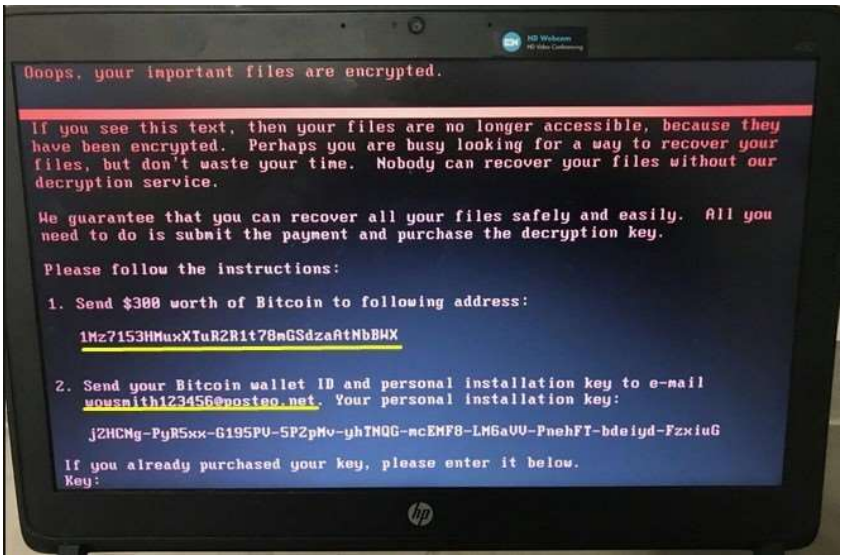




Screenshot: Bank Statement

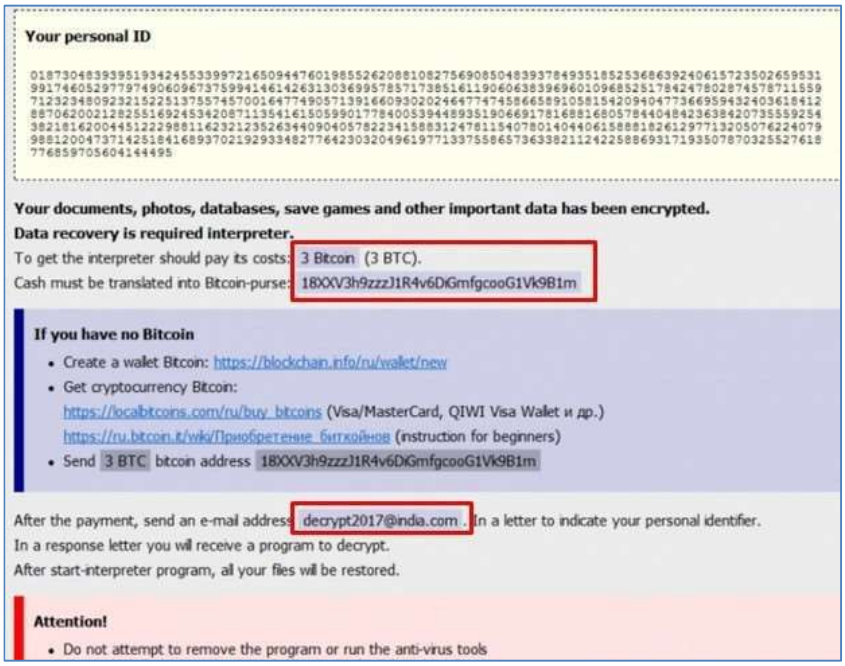
3.12 Sample Evidence for Ransomware

Following are some evidence samples which may be provided on the Ransomware category:



Payment details and Email

For example: BTC amount 3 BTC
BTC account address: 18XXV3h9zzz1R4v6DGmfgcooG1Vk9B1m
Email decrypt2017@india.com



Screenshot: Ransomware Details

3.13 Sample Evidence for Unauthorized Access Data/Breach

Following are some evidence samples which may be provided on the unauthorized access data breach category:

Example: Website URL: https://pastebin.com/0a4xKSn2

Screenshot: Website URL and content

3.14 Sample Evidence for Website Related/Defacement

Following are some evidence samples which may be provided on the website related/defacement category:

For example (Website URL: www.website.gov.in)

Screenshot: Website defacement upsc.gov.in

Other info: Mirror page of hacked website

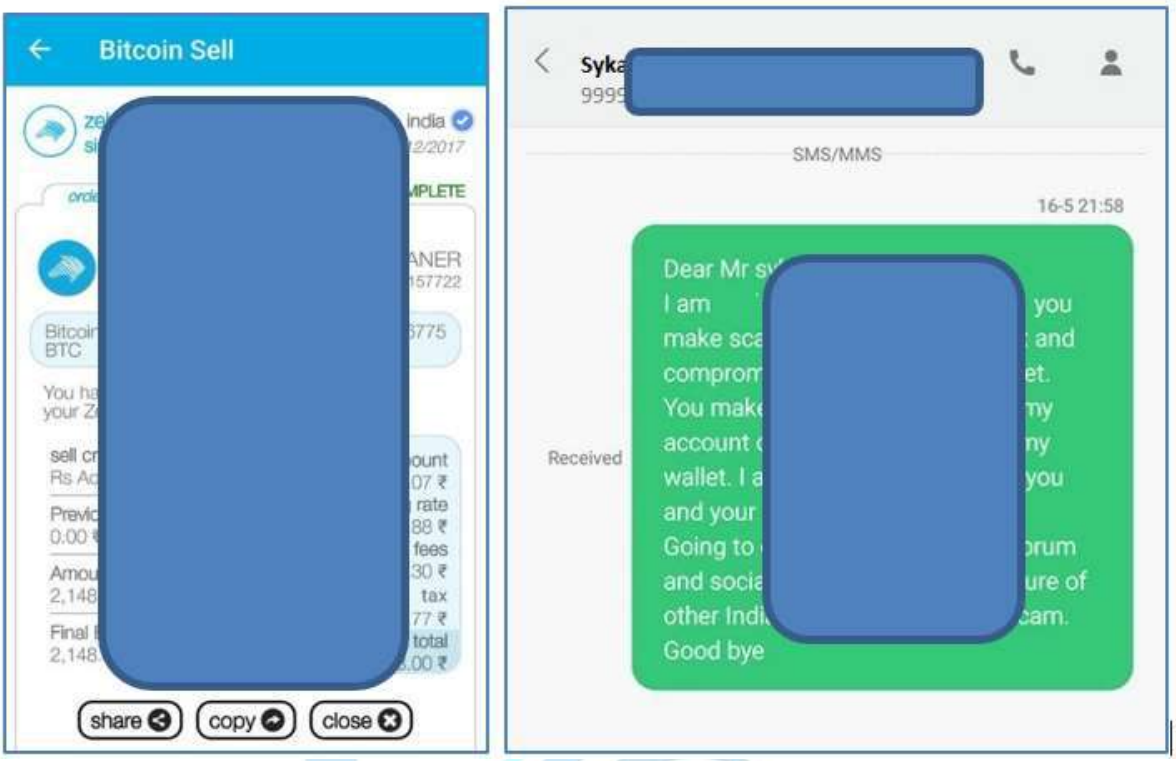
Screenshot: Mirror image of defaced website (website.gov.in) on zone-h

3.15 Sample Evidence for Cryptocurrency Fraud

Following are some evidence samples which may be provided on the cryptocurrency fraud category:

For example (Transaction details BTC address: 1FjqYtC3wwfzpAQDcRRTJRZguksfQRWeDq)

Sellers Btc Address : 1FjqYtC3wwfzpAQDcRRTJRZguksfQRWeDw
Seller business page https://www.facebook.com/wedvs



Snapshot: SMS Bitcoin details

3.16 Sample Evidence for Online Trafficking

Following are some evidence samples which may be provided on the online trafficking category:

*For example: UserID: seller userid, m**********g*

Messaging app: Instagram

Screenshot: User ID and Contact details

Screenshot: User ID