Documents Required for Reporting Online Cyber Crime

In Email related Complaints

- A written Complaint explaining the complete incidence
- Copy of the alleged Email
- Email should be taken from the original receiver. Copy of the forwarded email should be avoided
- Full Header of the alleged Email
- Copy of email and header should be in both hard & soft forms
- Soft copy should be given in a CD-R only

In Social Media related Complaints

- Copy/screenshot of alleged contents/profile
- Screenshot copy of URL of alleged contents
- Contents should be in both hard & soft forms
- Soft copy should be given in CD-R only

In Mobile Apps related complaints

- screenshot of the malicious app and the location from where it downloaded.
- Bank statement from the victim's account if any transactions are made.
- soft copy of all above mentioned documents in soft form

In Business Email Compromise complaints

Brief description of the incident, and consider providing the following financial information:

1. Originating Name
2. Originating Location
3. Originating Bank Name
4. Originating Bank Account Number
5. Recipient Name
6. Recipient Bank Name
7. Recipient Bank Account Number
8. Recipient Bank Location (if available)
9. Intermediary Bank Name (if available)
10. SWIFT Number
11. Date
12. Amount of Transaction
13. Additional Information (if available) - including “FFC”- For Further Credit; “FAV” – In Favor Of

In Data Theft complaints

- Copy of data which has been stolen
- Copyright certificate for the data in question.
- Details of the suspected employee who took the data from the company.

Following documents related to suspected employee:

- Appointment letter
- Non-disclosure agreement if any
- List of duties assigned.
- List of gadgets assigned to the suspected.
- List of clients with whom the suspect is in touch.
- Proof of selling your copyright data to any client.
- Devices used by the suspect while working with the company, if any.

In Ransomware complaints

- EMail id /phone number or any other means of communication through which ransom has been demanded.
- If malware was sent in the attachment of the mail. Screenshots of the mail with the full header of the first receiver should be provided.

In Net banking/ATM Complaints

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

In Fake call frauds

- Bank statement from the concerned bank of the last six months.
- 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.

In Lottery scams Complaints

- Bank statement from the concerned bank of the last six months.
- 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.

In Bitcoin related Complaints

- Complete facts in brief about the incident.
- Address of Bitcoin.
- Amount of Bitcoin involved.
- Address from/to whom purchase/sale of Bitcoins is done.

In Cheating related Complaints

- Print out of the alleged email along with its full header of the email
- Email should be taken from the original receiver.
- Copy of the forwarded email should be avoided
- Bank statement from the victim's account.
- Details of the alleged transaction made.
- Soft copy of all above mentioned documents.

In Online Transactions related Complaints

- Bank statement from the concerned bank of the last six months.
- 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.
- Fund receiver details like name, bank account , mobile number, email.
- Image of paytm or phonepe or google pay transaction receipt.