STANDING ORDER NO. 70 /2014

CYBER CRIME INVESTIGATION CELL, CHANDIGARH POLICE

PROCEDURE TO BE FOLLOWED WHILE ENQUIRING AND INVESTIGATING VARIOUS CYBER CRIME ISSUES IN THE JURISDICTION OF CHANDIGARH.

INTRODUCTION:

The total number of cyber related complaints have witnessed a quantum jump recently. Complaints are now being received directly as well as through emails. The sudden spurt in the number of complaints are mostly related to malicious content posted on social networking sites, fake email Ids, hacking of emails ids, hacking of websites, credit card frauds, internet banking etc. These complaints cannot be ignored because of the sensitivities involved. Many of these complaints are simple in nature and can be dealt with at the Police Station level as they do not require specialized investigation. With the Cyber Crime Investigation Cell, mandated to take up enquiries and investigations related to 'Serious cyber frauds', matters of data theft and other referred matters, the simple complaints and cases can be easily taken up at the Police Station level. Technical assistance, if any could be provided by the Cyber Crime Investigation Cell at Police Station Central, Sector 17, Chandigarh.

OBJECT:

The purpose of Cyber Crime Investigation Cell is to act as a catalyst in cases registered in various police stations under various sections of IT Act by providing necessary information for tracing the criminal through the cyber prints left by him while committing the crime. In addition to this, Cyber Cell will also investigate cases registered by Cyber Cell independently.

PROCEDURE FOR ENQUIRY / INVESTIGATION IN MATTERS RELATED TO SOCIAL NETWORKING SITES LIKE ORKUT, YOUTUBE, FACEBOOK, TWITTER ETC.

In such matters, the complainants and the victim are usually women. In some cases complaints are also given by the victim's father or other close relatives as the actual victim do not want to get themselves 6'4 identified due to personal/social reasons. These complaints relate to the creation of fake profile on social networking sites in the name of the victim, usage of personal photos, name, personal phone number of friends and family of the victims. Sometimes fake sexually explicit profiles are created and phone numbers are put on adult sites to harass the victims. These profiles as well as the contents of such sites are generally offensive, derogatory and lascivious. On receipt of a complaint related to hosting of a fake profile on any social networking site, the following procedure has to be followed.

1. A full printout of the fake profile with full URL has to be taken and downloaded from the site.
2. A copy of the offending profile with full URL has to be saved electronically on a computer.
3. The IC of the concerned case should send a DO Letter as per the specimen letter, under the signature of the authorised signatory in electronic form to the concerned Service provider for following:
   a. Registration and Login details of the offending profile from the concerned social networking site.
   b. A request also be sent for blocking or removing the offending profile if the complainant so desires.
   c. Details of the location including address of the various logins from the concerned Internet Service Provider (ISP).
   d. Registrant login details, if possible, of the email id Used to create the profile.
   e. Details of the location, including address of the various logins from the related Internet Service Provider (ISP) of the concerned-email address (email ID).

PROCEDURE FOR ENQUIRY / INVESTIGATION IN MATTERS RELATED TO HACKING/UNAUTHORIZED ACCESS INTO EMAILS:

In such matters the complainant alleges that his/her email account, which is generally created on a free portal, has been hacked. The complainant complains that he/she is not able to access his/her account. At times it is also mentioned that someone else is sending mails from the hacked email account. On receipt of a complaint of such a matter, the following procedure has to be followed:-

1. In cases where the complainant claims that the hacker is sending malicious emails from the victim's account, a copy of the full header as well as the text of the email, both in the printed form as well as in an electronic form has to be collected from the recipient of such emails.
2. The said complaint along with the copies of full header, if any, is to be analyzed and the following information should be sought:-
   a. The internet protocol (IP) address, date and time of the received email as revealed by the header.
   b. The IP usage details including the geographical address of the disclosed IP address, from the concerned Internet Service provider (ISP).
   c. All the login details of the hacked email address (email ID) from the portal where the said email account has been hosted.
   d. The access details, IP addresses, date and time when the hacked email account has been accessed and when the passwords have been changed.
   e. The usage details of the said IP addresses from the concerned ISPs.
PROCEDURE FOR ENQUIRY / INVESTIGATION IN MATTERS RELATED TO 419 SCAMS OR "CRIME OF PERSUASION".

In such matters the complainants allege that they have received emails from unknown sources wherein they have been informed that:

1. Either they have won a lottery worth lacs of rupees & millions of dollars or
2. Their help is required for transferring illegal money from some African Country or
3. They have been selected for an overseas job, generally a hotel job in some European/American country or
4. Goods are offered at throw away prices or
5. They have been granted a loan or
6. The victims address book in their emailing list is compromised and emails are sent to all their contacts from their ID asking for money to bail them out from a perilous situation.

The complainant is trapped in a phased manner and is generally made to deposit a huge amount of money either as money transfer fee, payment of taxes or transportation cost etc. The complainant apparently receives a spam email and responds to the same and ends up paying money to some unknown persons for a non-existent purpose. Such crimes are invariably carried out from abroad. Money is either deposited in offshore accounts or some courier account in India. On registration of a case or receipt of complaint in such matters, the following procedure has to be followed:-

1. Printouts of emails (both sent and received by the complainant) with full email headers, have to be collected.
2. Assistance can be taken from the Cyber Crime Cell in tracing the origins of these emails.
3. Copies of these emails have to be saved electronically on a computer.
4. The intermediate beneficiary or courier bank account has to be traced through the details mentioned in the bank account opening form and for from the mobile numbers, if available. This has to be done immediately without loss of time.
5. The debit of the intermediate account has to be frozen.
6. The customer form and call records of the mobile phone being used to contact the complainant to be collected and be analyzed to trace the alleged person(s).
7. Alternatively traps can be laid and the intermediary may be called in person for a meeting to collect the money.
8. If computers/hard disks, laptops, mobiles are seized, they can be sent to Andhra Pradesh Forensic Science Laboratory, Hyderabad or Forensic Science Laboratory, Gandhi Nagar, Gujarat or Central Forensic Science Laboratory, Chandigarh or any other authorized laboratory for analysis and report.
PROCEDURE FOR ENQUIRY/INVESTIGATION IN MATTERS RELATED TO UNAUTHORIZED ONLINE TRANSACTIONS THROUGH CREDIT CARDS.

In such matters, the complainant alleges that some unknown person had withdrawn money/made transactions through his/her credit cards through online purchasing. In most of these cases purchasing is done by using the crucial information of the credit card viz a) 16 Digit Credit Card Number; b) validity of the credit card; c) 3 digit confidential Card verification Value (CVV) for the completion of the transaction. Any person having these three information of the credit card can make the transaction without having the knowledge of the credit card holder. Generally, the credit limits of these cards are high and the matters is disclosed to the actual owner of the card when he/she receives the account statement of the card from the banking agency or an SMS about the transaction.

In such matters the following procedure should be adopted:

1. The credit card holder should be asked to immediately lodge a complaint with the concerned bank.
2. Information about the card usage history be obtained from the complainant to find the clues about the possible source of compromise of the credit card information.
3. The account statement of the credit card indicating the illegal transaction should be obtained from the complainant/bank.
4. Information should be collected from the concerned bank regarding the mode/description of the transaction and the details of articles/items purchased along with the details of the email ID used by the suspect.
5. The IP address of the suspect, through which the transaction was carried out, be obtained from the merchant/bank to locate the physical address of the user.
6. The EO/IO should then obtain the following information:
   a. The usage details of the IP address provided by the bank
   b. The registrant and login details of the email ID used by suspect from the concerned service provider.
   c. The geographical address For the IP logs so obtained, from the concerned ISP.
7. In cases where an air ticket has been purchased, the PIN number of the ticket booked and the details of the passenger traveling on the said ticket should be obtained from the concerned Airlines.
8. Assistance of the bank's Fraud and Risk Management team should also be sought for tracing the credit card usage.
9. In case computer/hard disks, Laptops-etc. are seized they should be sent to FSL for analysis and report.

PROCEDURE FOR ENQUIRY IN MATTERS OF WEBSITE HACKING:

In such matters the complainant alleges that some unknown person has hacked the admin panel of their website and has changed the contents/images of website. The following procedure has to be adopted in such matters:-
1. Get the name of file/webpage from the website administrator which was placed by the hacker on the website.
2. Obtain exact date and time at which the hacking took place from the administrator of the website.
3. Obtain IP address from website administrator from which the hacking took place.
4. Admin Logs should be obtained from the complainant/Host server of the date on website hacking took place.
5. FTP Logs to be obtained from the complainant/Host server of the date on which the hacking-took place.
6. Copy of entire contents uploaded on website during the hacking period, should be taken from the complainant as proof of hacking.
7. The usage details of the said IP addresses should be collected through the concerned ISPs.

**PROCEDURE FOR INVESTIGATION IN MATTERS RELATED TO INTERNET BANKING FRAUDS:**

In such matters, the complainant alleges that some unknown person had transferred money from complainant's account to other accounts using Internet banking. In these cases complainant's Internet password may be procured through phishing by the fraudster. Alternatively, the internet banking password could be compromised through the second step verification process i.e. OTP (One Time Password) which is invariably delivered on the user's authorized Mobile number. In this modus operandi the fraudster invariably gets the original SIM blocked and obtains a duplicate SIM in place of the original one with the help of fake documents.

In such matters the following procedure should be adopted:

1. The Account holder or the complainant should be asked to immediately lodge a complaint with the concerned bank.
2. Information about the Account statement to be obtained from the complainant to find beneficiaries’ accounts.
3. The account statement, account opening form and other details related to complainant account should be obtained from the concerned bank.
4. The account statement, account opening form and other details related to beneficiaries’ account should be obtained from the concerned bank.
5. The beneficiaries' accounts should be blocked immediately.
6. The IP address of the suspect through which the transaction was carried out be obtained from the bank.
7. Details of the geographical address for the particular IP usage should be obtained from the ISP concerned.
8. The EO/IO can seek the assistance from the Cyber Cell to obtain the following information:–
   a. The usage details of the IP address provided by the bank.
   b. The registrant and login details of the email ID used by suspect from the concerned service provider.
c. The geographical address for the IP logs so obtained, from the concerned ISP.

9. The CDRs, CAF, IMEI, IMSI details of the mobile numbers mentioned in AOF of the beneficiaries' accounts should be obtained from the service providers.

10. Assistance of the bank's Fraud and Risk Management team should also be sought for tracing the account usage.

11. In case computers/hard disks, Laptops etc. are seized they should be sent to Andhra Pradesh Forensic Science Laboratory, Hyderabad or Forensic Science Laboratory, Gandhi Nagar or Central Forensic Science Laboratory, Chandigarh or any other any Govt. authorized laboratory for analysis and report.

PROCEDURE FOR ENQUIRY / INVESTIGATION IN PLATTERS RELATED TO DEFAMATORY, THREATENING AND ABUSIVE EMAILS:

In such matters the complainant alleges that he/she has received a defamatory, threatening and/or abusive email in his/her emails account. On receipt of a complaint of such nature, the following procedure has to be followed:-

1. A copy of the full header as well as the text of the said email, both in the printed form as well as in an electronic form has to be collected from the recipient of such email.

2. The said complaint along with the copies of full header, if any, is to be analyzed and information sought as follows:-

   a. The Internet protocol (IP) address, date and time of the received emails as revealed by the header.
   b. The IP usage details including the geographical address of the disclosed, IP address, from the concerned Internet Service provider (ISP).

3. The registrant details, log details (including IP addresses and data/time) of the email ID from where the offending email has been received, to be obtained from the portal where the said email account has been-hosted.

4. The usage details of the said IP addresses obtained from (4) above be obtained from the concerned ISPs.

PROCEDURE FOR COLLECTION INFORMATION/EVIDENCE FROM ABROAD:

In many Cyber investigations, information / evidence in the form of information content; registrant details, usage details, server logs etc have to be obtained from abroad. However, it may not be necessary to gather formal evidence in all such cases; the investigation may need only some information or a lead in the first instance. Thus, besides the Formal Investigation Requests, information can also be obtained through the faster Informal Investigations Requests. The process of informal and the formal investigation requests are details below:
1. **Informal Investigation Requests**: The process to be followed to obtain information informally from the National Central Bureaus of other countries, through the Interpol channels as well as Indian Missions (embassies, consulates and high commissions) abroad as follows:

   a. A self-contained request, along with necessary details, should be addressed to Asstt. Director, International Police Cooperation Cell, (IPCC), 5th floor, CBI Headquarters, Plot No. 5B, CGO complex, Lodhi Road, New Delhi.

   b. In case, the requisite information to be collected/enquiries to be conducted are in more than one country, separate self-contained requests may be sent for each country.

   c. The self-contained request must incorporate the following details:

      i. The FIR No. along with names of the accused and sections of laws under which the case has been registered:

      ii. The gist of allegations in the FIR/ Preliminary Enquiry or any other investigation process.

      iii. The details of information required. In order to make the task of the requested country easy, specific relevant details must be furnished.

**INVESTIGATION:**

Every complaint related to cyber crime will be dealt by Cyber Crime Investigation Cell after duly received through Centralized Public Window System. An FIR will be registered after proper enquiry and after prior approval of SSP/UT. SSP/UT shall keep IGP informed about the registration of case.

   i) In case after the preliminary enquiry no cognizable offence is made out, a report sent to the SSP for final orders and disposal.

   ii) A weekly report for the progress of cases and pending complaints shall be sent by the Inspector/Incharge through the DSP/CCIC.

➢ The help of experts in the field of cyber crime and investigation continuously will be taken by the Cyber Crime Investigation Cell from time to time.

➢ Cyber Crime Investigation Cell will continuously endeavor to create awareness among the general public regarding cyber crime.

**STRENGTH**

The strength of the Cyber Crime Investigation Cell will be as under:-

   i) Dy. Superintendent of Police (1)
   ii) Inspectors (4)
   iii) Sls/ASls (8)
iv) Head Constables (12)
v) Constables/Lady Constables (20)
vi) Driver Constables (5)
vii) Home Guard Volunteers (5)

RECORD/ REGISTERS:

The following record/ registers shall be maintained by this wing:

i) DAILY DIARY

A daily Diary register shall be maintained in form 22.48 (1) in duplicate by carbon copy process. The staff while taking over duties will sign the entries made in the daily dairy regarding the same. The daily diary shall be a complete record of all important proceedings and duties and movements of the personnel of Cyber Crime Investigation Cell. All entries regarding arrests of the accused and information, regarding arrest given to relatives, control room as per various guidelines issued by the Police Headquarters shall be duly entered in the daily dairy. The Inspector- Incharge will ensure that correct entries are made in the daily diary and it is nearly maintained. The carbon copy shall be submitted to the DSP- Incharge of the unit, after it is closed for the day for his information and further action.

ii) STANDING ORDER FILE

A file shall be maintained in which orders and instructions received from senior officers shall be filed.

iii) DESPATCH AND RECEIPT REGISTER

A register in the prescribed form for Police Station Register No.5 shall be maintained for the entry of dispatch and receipt of all kinds of orders, complaints and miscellaneous dak etc.

iv) REGISTER NO.16

A register in the form No. 16.5(1) shall be maintained regarding the profiles/contact information of the posted officials with the cyber crime investigation cell.

v) DAK BOOK

A dak book shall be maintained which shall contain entries about the dak dispatched from the unit. The signatures of the person receiving the dak, shall be obtained on the dak book.

vi) MISCELLANEOUS FILES

All miscellaneous papers shall be filed in the miscellaneous file maintained in the unit.
VEHICLE:

MTO shall provide vehicles with driver for official duties for effective functioning of the wing.

ARMS AND AMMUNITION:

Arms and Ammunition, as and when required by the staff for official duties, shall be drawn from Police Station Sec-17 and shall be deposited back after the duty is over.

INTEGRITY & COMMITMENT:

The Cyber Crime Investigation Cell will endeavor to achieve all the above objectives with integrity and commitment, in keeping with the highest traditions & values of the Chandigarh Police.

TRAINING:

It will be imperative on the part of DSP Cyber Crime to organize specialized courses and workshops for imparting training to officials working in Cyber Crime Investigation Cell.

SUPERVISION:

The Cyber Crime Investigation Cell shall function under the supervision of DSP, who shall report to SSP/UT and ensure that CCIC works towards the objective and detection of cyber crime related offences.

This standing order supersedes the previous standing orders issued in this regard, if any.

(R.P. Upadhyay), IPS,
Inspector General of Police,
UT, Chandigarh

No. 29344-80/UT/E6 dated, Chd, the 13th June, 2014

All. Conceded:— I/C Computer Section