# The Complete Post-Complaint Manual for Every Cybercrime in India

After filing a complaint on the cybercrime portal and receiving your acknowledgment number, the journey towards resolution begins. While the core process of police inquiry and investigation remains the same, the specific actions you need to take vary depending on the nature of the crime. This manual details the crucial next steps for different categories of cybercrime.

## Part A: For Crimes Against Women & Children

This includes cyberstalking, online harassment, morphing (altering photos), sextortion, trolling, and circulation of Child Sexual Abuse Material (CSAM). These cases are treated with high priority and sensitivity.

**Phase 1: Immediate Next Steps (Your First 24 Hours)**

1. **Prioritize Safety & Preserve Evidence:**
    - **Do Not Engage:** Stop all communication with the perpetrator immediately. Do not respond to threats or provocations.
    - **Secure Digital Evidence:** Take screenshots of everything – chat messages, profiles, comments, images, videos, and URLs. Do not delete or alter anything. If possible, use another device to photograph the screen displaying the content.
    - **Secure Your Accounts:** Immediately change your passwords for all social media and email accounts. Strengthen your privacy settings to the maximum level (e.g., make your profile private, limit who can see your posts and friend list).
    - **Inform a Trusted Adult:** If you are a minor, it is imperative to inform a parent, guardian, or trusted teacher immediately.
2. **Special Reporting Options:**
    - The portal (cybercrime.gov.in) has a dedicated option to **"Report Women/Child Related Crime"** which allows for anonymous reporting. Even if you have already filed, be aware of this for future reference.
    - Your complaint is routed with high priority to the respective state's police force for immediate action.

**Phase 2: During the Investigation**

1. **Cooperation with Law Enforcement:**
    - The police will likely contact you. Be prepared to provide a detailed statement in a safe and comfortable environment. For women, this can be done in the presence of a female police officer.
    - Hand over all the evidence you have collected. The police need this to build a strong case.

    - In cases involving the **POCSO Act (Protection of Children from Sexual Offences Act)**, the investigation is highly sensitive and legally bound to be child-friendly and confidential.
2. **Your Rights and Support:**
    - **Right to Confidentiality:** Your identity will be kept confidential throughout the investigation and trial process.
    - **Seek Psychological Support:** Dealing with such crimes is traumatic. Contact government or NGO-run helplines for counseling and support. (e.g., NIMHANS Centre for Well-Being, various women's helplines).

---

## Part B: For Financial Frauds

This includes UPI fraud, credit/debit card fraud, phishing scams, e-wallet fraud, and ransomware attacks. **Time is the most critical factor here.**

**Phase 1: Immediate Next Steps (The "Golden Hour")**

1. **Call Helpline 1930 Immediately:**
    - Even before or right after filing on the portal, **call the Citizen Financial Cyber Fraud Reporting and Management System at helpline number 1930**.
    - This is the most crucial step. Provide them with your transaction details (Transaction ID, date, time, amount) and details of the fraudulent account.
    - The helpline immediately triggers an alert to the concerned banks, e-wallets, and merchants to attempt to block the transfer of money. This "Golden Hour" is your best chance to recover the funds.
2. **Contact Your Bank/Financial Institution:**
    - Simultaneously, call your bank's official customer care number. Inform them about the fraudulent transaction.
    - Request them to immediately freeze your account, block your card, and initiate a "chargeback" if applicable (especially for credit card transactions).
    - Formally report the fraud in writing by sending an email to your bank's grievance redressal cell. Attach a copy of your police complaint from the portal.

**Phase 2: During the Investigation**

1. **Document Everything:**
    - The police and the bank will require documents. Keep soft and hard copies of:
        - Bank statements highlighting the fraudulent transaction.
        - The SMS and email you received for the transaction.
        - Your complaint acknowledgment number.
        - All communication (emails, chats) with the fraudster.
2. **Follow Up Consistently:**
    - Regularly follow up with your bank on the status of your dispute.
    - Stay in touch with the investigating officer for updates on the case.

---

## Part C: For Matrimonial & Job Frauds

These crimes often involve emotional manipulation leading to financial loss.

**Phase 1: Immediate Next Steps**

1. **Cease All Contact & Secure Evidence:**
    - Stop communicating with the fraudulent individual or "company."
    - Secure all evidence: the matrimonial or job portal profile, all chat conversations (WhatsApp, Telegram), emails, phone numbers, and any documents they sent you (fake offer letters, ID cards).
    - Document all financial transactions, including bank account details to which you sent money.
2. **Report to the Platform:**
    - In addition to the police complaint, report the fraudulent profile to the grievance officer of the matrimonial site or job portal. This helps them take down the profile and prevent others from becoming victims.

**Phase 2: During the Investigation**

1. **Provide Detailed Context:**
    - The police will need the full story. Be prepared to narrate the entire sequence of events, from initial contact to when you realized you were being cheated.
    - Provide the list of phone numbers, bank accounts, and profiles used by the fraudster.
2. **Connect with Other Victims (If Possible):**
    - Often, these fraudsters cheat multiple people. Sometimes, a simple social media search reveals other victims. Sharing information (under the guidance of the police) can strengthen the case.

---

## Part D: For All Other Cybercrimes

This is a broad category including social media impersonation, cyber defamation, email hacking, data theft, and online threats.

**Phase 1: Immediate Next Steps**

1. **Report on the Specific Platform:**
    - **Impersonation/Fake Profile:** Use the "Report" feature on Facebook, Instagram, Twitter, etc., to report the fake profile for impersonation. The platform's own moderation is often the fastest way to get a fake profile taken down.
    - **Defamation:** Report the defamatory post or comment directly to the platform.
    - **Hacked Account:** Use the platform’s account recovery feature immediately to try and regain control.

2. **Preserve and Protect:**
    - Take screenshots and record URLs of the offending content. For defamation, evidence is key.
    - Inform your friends and contacts from a genuine account that your profile has been compromised or impersonated to prevent them from being cheated.
    - If your email is hacked, immediately change the passwords of all linked accounts (banking, social media, etc.) as they are now vulnerable. Enable Two-Factor Authentication (2FA) everywhere.

**Phase 2: During the Investigation**

1. **Provide Technical Details:**
    - For hacking cases, the police may need technical details like email headers to trace the origin of a message. Be prepared to provide access or information as guided by them.
    - For data theft, you may need to detail exactly what information was stolen.
2. **Follow Up on Content Takedown:**
    - The police can issue legal notices (under Section 79 of the IT Act) to social media companies and internet service providers to take down malicious content and provide user details of the accused. Follow up with the investigating officer on the status of these notices.