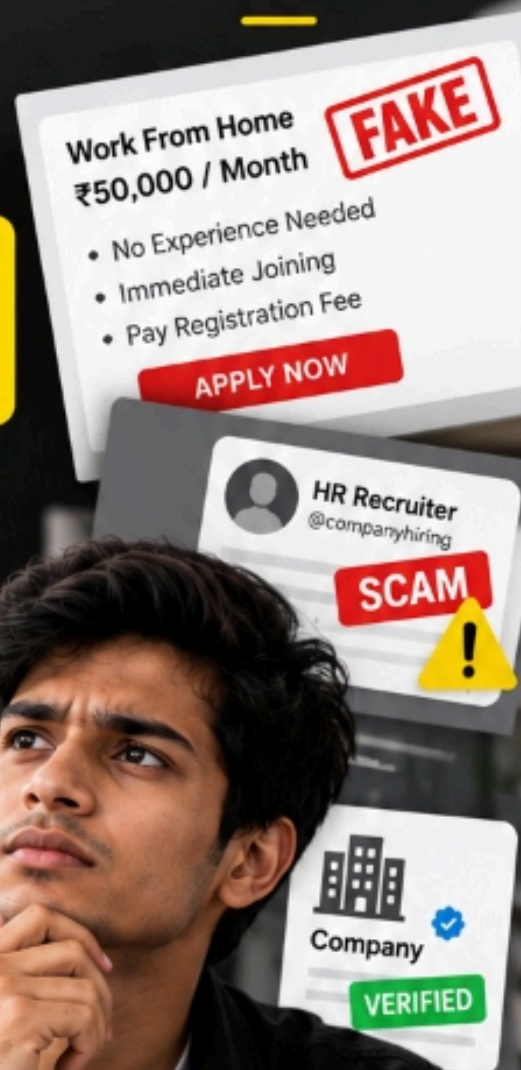


JOB VERIFICATION & SCAM PROTECTION GUIDE

How to Identify Fake Job Postings, Verify Recruiters, Avoid Payment Scams and Protect Your Personal Data.

- ✓ Spot Fake Job Listings
- ✓ Verify Companies and Recruiters
- ✓ Avoid Common Scams
- ✓ Protect Your Personal Data
- ✓ Safe Job Search Practices



SAFE
SEARCH
BETTER
OPPORTUNITIES



FAKE JOB
POSTINGS



RECRUITER
VERIFICATION



PAYMENT
SCAMS



PERSONAL DATA
PROTECTION



SAFE JOB
SEARCH TIPS

Table of Contents & Executive Briefing

Employment scams in India have evolved from crude roadside flyers into sophisticated digital syndicates operating across WhatsApp, Telegram, professional networking sites, and fake corporate portals. This handbook equips you with systematic, field-tested verification habits.

GUIDE CONTENTS

- **Chapter 1:** How to Identify Fake Job Postings
- **Chapter 2:** How to Verify Recruiters and Company Profiles
- **Chapter 3:** How to Check Whether a Job Offer Is Genuine
- **Chapter 4:** Registration Fees & Advance Payment Scams
- **Chapter 5:** Suspicious Links & Personal Data Protection
- **Chapter 6:** Recruiter Verification Checklist & Framework
- **Case Studies:** 5 Realistic Illustrative Scams Analyzed
- **Emergency Response:** Immediate Actions for Fraud Victims
- **Directory:** Official Indian Verification & Reporting Channels

TARGET AUDIENCE

Written specifically for the Indian job ecosystem:

- **College Freshers & Students:** Stepping into off-campus placements.
- **Experienced Professionals:** Safeguarding against executive headhunter impersonations.
- **Unemployed & Career Returners:** Guarding against urgent, high-stress offers.
- **Remote & WFH Seekers:** Defending against task/review frauds.

THE ABSOLUTE FUNDAMENTAL LAW OF RECRUITMENT

Legitimate employers pay you for your talent, time, and work. They never ask you to pay them for the opportunity to work. If anyone asks for money before or after hiring you, pause immediately.

How Modern Employment Fraud Operates in India

Recruitment fraud relies on three psychological levers: **Urgency** (making you act before thinking), **Authority** (using famous brand logos and corporate names), and **Relief** (promising instant financial stability). When you understand these tactics, fraudsters lose their power over you.

CORE SAFETY PRINCIPLES BEFORE YOU BEGIN

- ✓ Treat any unsolicited offer delivered directly via SMS, WhatsApp, or Telegram with healthy skepticism.
- ✓ Never transfer funds via UPI or bank deposit for registration, interview slots, uniforms, or laptop security.
- ✓ Always perform independent research using official corporate websites and public government registries.

CHAPTER 1

How to Identify Fake Job Postings

Fraudulent job postings are widespread across public job aggregators, classified boards, Telegram channels, and social media feeds. They are crafted to attract maximum applicants by offering maximum reward for minimal effort.

Primary Warning Signs in Job Listings

- **Unrealistic Compensation Promises:** Offering ₹35,000 to ₹75,000 per month for basic data entry, SMS forwarding, or copy-paste assignments with "no qualifications required." Real market pay reflects actual skill requirements and economic output.
- **Vague Roles & Responsibilities:** The listing uses ambiguous buzzwords: "Online computer operator," "Part-time digital partner," "2-3 hours daily from mobile." Legitimate postings clearly list specific responsibilities, reporting structure, and required tools.
- **Suspicious Application Channels:** Instead of directing applicants to an ATS (Applicant Tracking System), LinkedIn job portal, or corporate career URL, the listing urges: "Send resume on WhatsApp 98XXXXXXX" or provides a direct link to an anonymous Telegram handle.
- **Copied Content & Poor Grammar:** Stolen job descriptions with mismatched font styles, strange spelling errors, outdated logos, or conflicting company names in the body text.
- **Work-From-Home (WFH) Red Flags:** High-risk remote listings often demand that candidates install third-party `.apk` applications or promise "daily UPI earnings" for reviewing products and liking videos.

WARNING: THE "DAILY TASK" SCAM TRAP

Fraudsters often pose as global e-commerce or digital marketing agencies offering "Work From Home" tasks. They pay small real rewards (₹150–₹500) initially to build trust, then demand deposits of ₹5,000 to ₹50,000 to "upgrade your task tier." This is an investment fraud known as the *Task/Recharge Scam*.

WHAT TO DO NEXT (CHAPTER 1 ACTION CHECKLIST)

- ✓ Examine the job description: Are technical qualifications, education, and specific duties explicitly stated?
- ✓ Copy a paragraph of the job description into Google search to verify if it was copy-pasted from an authentic opening.
- ✓ Refuse to continue if the applicant is instructed to converse solely via personal WhatsApp or Telegram handles.
- ✓ Never install `.apk` files or proprietary software sent over private messaging chats.

Evaluating Job Advertisements: Side-by-Side Analysis

Examine this practical side-by-side comparison to train your eye in spotting subtle red flags before spending time applying.

EVALUATION METRIC	SUSPICIOUS LISTING (HIGH RISK)	CREDIBLE LISTING (STANDARD PRACTICE)
Salary & Payout	"Earn ₹2,000–₹5,000 daily! Guaranteed payout every evening via Google Pay/PhonePe. No targets!"	"CTC: ₹3.6 LPA – ₹4.8 LPA, based on technical assessment and past relevant experience."
Job Description & Scope	"Simple work-from-home typing. Any 10th/12th pass can do. Basic mobile phone needed. No experience."	"Customer Support Specialist: Requires fluency in English & Hindi, CRM management, ticket escalation, 40 WPM typing speed."
Application Gateway	"Don't send email. Click wa.me/91XXXXXXX to chat directly with Madam Pooja on WhatsApp."	"Apply via corporate careers portal: careers.companyname.com or verified LinkedIn Easy Apply."
Email & Domain	Contact email listed as: <code>`tatamotors_recruitment2026@gmail.com`</code> or <code>`info@reliance-hiring.xyz`</code> .	Official corporate domain: <code>`talentacquisition@tatamotors.com`</code> or matching website URL.
Selection Method	Immediate confirmation without an interview: "Congratulation! Your resume selected. Join today."	Structured multistage evaluation: HR screening, technical assessment, manager interview round.

Red Flag Visual Patterns

- Excessive emojis (🔥 🔥 💰 💰) in corporate job announcements.
- Low-resolution, stretched, or outdated corporate brand logos.
- Aggressive urgency: *"Hurry! Only 5 vacancies left today!"*
- Lack of a registered corporate headquarters address.

Credible Visual Patterns

- Clear Requisition ID / Job Reference Code.
- Professional corporate email and transparent team information.
- Structured overview of company culture and benefits.
- Documented grievance and diversity policies.

KEY TAKEAWAY

Scammers prey on job-search fatigue. If a job posting sounds too convenient, pays far above market rates, and requires no demonstration of competency, pause immediately. Real employers test your abilities before offering you their money.

CHAPTER 2

How to Verify Recruiters & Company Profiles

In modern recruitment, anyone can download a corporate logo, create a social media profile, and claim to be a "Senior Talent Acquisition Manager." Verifying the human and the company behind the message is your primary security firewall.

1. Check the Company's Official Web Presence Independently

Never click the links provided inside the recruiter's message or email. Open an independent browser window, search for the company name, and navigate to their official website. Look for:

- An active, well-maintained corporate domain with an SSL certificate (https://).
- A verifiable physical registered office address and working corporate landline numbers.
- Active registration on the Ministry of Corporate Affairs (MCA) portal ('mca.gov.in') with a valid Corporate Identification Number (CIN) or LLPIN.

2. Scrutinize Email Domains & Impersonation Techniques

Email is the easiest channel to spoof if you do not pay attention to the exact domain suffix:

DOMAIN CATEGORY	EXAMPLES	SAFETY VERDICT
Free Public Webmail	`recruiter.infosys@gmail.com`, `hr_wipro@yahoo.com`	EXTREME DANGER: Real enterprises never hire via free email.
Typosquatting Domains	`hr@wipr0.com`, `careers@tcs-careers-india.com`	SCAM DOMAIN: Lookalike domains created to trick the eye.
Authentic Corporate Domain	`recruitment@wipro.com`, `careers@tcs.com`	LEGITIMATE: Matches verified company website.

3. Why Logos and Polished Profiles Prove Nothing

A professional headshot, detailed career history, and high follower count on LinkedIn or Telegram do not guarantee authenticity. Scammers routinely clone existing HR professionals' profiles by copying their photos and employment history.

WHAT TO DO NEXT (CHAPTER 2 ACTION CHECKLIST)

- ✓ Inspect the sender's exact email address—examine every letter after the '@' symbol.
- ✓ Search for the recruiter on LinkedIn and send a direct InMail message to verify they actually sent the email.
- ✓ Search for the job Requisition ID directly on the company's official careers page ('companyname.com/careers').
- ✓ Call the company's official landline switchboard to verify the recruiter's employment status.

CHAPTER 3

How to Check Whether a Job Offer Is Genuine

An official offer letter or Letter of Intent (LOI) represents a formal employment contract. Scammers generate attractive appointment letters featuring forged signatures, counterfeit corporate stamps, and government emblems to deceive candidates.

Anatomy of a Genuine Indian Employment Offer

A legitimate formal offer letter from an established Indian employer contains clear, standardized legal and financial components:

Legitimate Offer Essentials

- Full legal entity name, CIN, and registered address.
- Detailed CTC annexure with Basic, HRA, PF, and deductions.
- Clear probationary term, leave policy, and notice period.
- Authorized corporate signatory with formal title.
- Standard documentation requirements (PAN, Aadhaar, marks).

Fraudulent Offer Indicators

- Flat lump-sum salary with zero statutory deduction breakdown.
- Counterfeit government seals or arbitrary "Ministry" stamps.
- Clauses demanding payment for laptop, uniform, or verification.
- Signatory contact info lists a mobile number or '@gmail.com'.
- Ultimatums: *"Sign and pay within 4 hours or offer is cancelled."*

The High-Pressure Deadline Trap

Scammers create artificial emergencies: *"Your selection expires at 5:00 PM today! Pay the registration fee immediately to lock your seat."* Reputable employers provide 3 to 7 working days for candidates to review the terms, consult mentors, and accept the offer. Pressure to act within hours is a universal red flag.

The "Direct Selection Without Interview" Fallacy

If you receive an offer letter without ever participating in a live video, telephone, or in-person evaluation with functional interviewers, **it is fraudulent**. Enterprises invest time and money into finding qualified talent; no company hires blindly.

WHAT TO DO NEXT (CHAPTER 3 ACTION CHECKLIST)

- ✓ Did you undergo real, comprehensive interview rounds? If not, treat the offer with extreme suspicion.
- ✓ Review the CTC annexure: Does it calculate Provident Fund (PF) and Professional Tax (PT) correctly?
- ✓ Never verify an offer letter using contact details printed on the letter itself. Find contact info independently.
- ✓ Email the corporate HR department ('careers@company.com') with the job reference ID to confirm authenticity.

CHAPTER 4

Registration Fees & Advance Payment Scams

Demanding upfront money under fabricated excuses is the core objective of 90% of employment scams in India. Once money is transferred via UPI or IMPS, recovering it is extremely difficult.

Common Excuses Scammers Use to Demand Money

- **"Registration & Processing Fee":** "Pay ₹1,200 to register your profile in our internal candidate portal." In reality, legitimate recruitment consultancies are paid by the hiring companies, not candidates.
- **"Refundable Laptop / Asset Deposit":** "Pay ₹5,000 as security for your company laptop and broadband kit; 100% refunded on Day 1." Real companies handle equipment distribution at their own expense.
- **"Mandatory Onboarding Training / LMS Fee":** "Deposit ₹7,500 for a mandatory 5-day corporate certification before joining." Authentic corporate training is funded entirely by the employer.
- **"Medical Examination / Background Verification Fee":** Directing candidates to pay a specific unverified clinic or agency for background verification.
- **"Guaranteed Job / Interview Slot Fee":** Asking for money to "guarantee" a job or secure an interview with senior executives.

CRUCIAL DISTINCTION: LEGITIMATE EXPENSES VS. FRAUDULENT FEES

Legitimate: Public Sector / Government exam application fees (UPSC, SSC, IBPS, Railways) paid strictly through official `.gov.in` / `.nic.in` gateways. Your own personal travel expenses to attend an in-person interview.

Fraudulent: ANY demand by a private company, consultant, or agency for money as a condition for interviewing, receiving an offer letter, dispatching hardware, or joining.

How to Handle an Upfront Payment Request

1. **Refuse immediately:** Politely decline: "As per standard recruitment practice, I do not pay advance fees for employment."
2. **Request official written policy:** Ask for company policy on official letterhead from a corporate domain email.
3. **Preserve all evidence:** Save screenshots of payment QR codes, UPI IDs, and chat messages.

WHAT TO DO NEXT (CHAPTER 4 ACTION CHECKLIST)

- ✓ Commit to the Zero Upfront Fee rule: Never pay any private recruiter or employer.
- ✓ If a recruiter asks for money, immediately freeze all communication and block the number.
- ✓ Take screenshots of the UPI ID, phone number, and conversation before blocking.
- ✓ Report the fraudulent profile on the platform where they first contacted you.

CHAPTER 5

Suspicious Links & Personal Data Protection

Employment fraud is not only about stealing money directly. Criminals also harvest identity documents and banking credentials to execute bank fraud, take out unauthorized loans, or open fraudulent SIM cards in your name.

1. Recognizing Phishing Forms & Malicious Links

Scammers share Google Forms, Typeforms, or lookalike web portals titled *"Employee Onboarding & Salary Account Verification."* These forms request sensitive information:

- Bank account credentials, internet banking usernames, passwords, or transaction PINs.
- Credit / Debit card numbers, expiry dates, and 3-digit CVV codes.
- Requests to download and install custom Android applications (`.apk` files) or PC software (`.exe`).

The Threat of Malicious APK Files

Never install an `.apk` file sent via WhatsApp or Telegram. These applications often contain remote-access trojans (RATs) or SMS forwarders that intercept your bank OTPs silently in the background, allowing hackers to drain your bank account within minutes.

2. Best Practices for Sharing Indian Identity Documents

While legitimate employers require identity proof for payroll and PF registration, you can protect yourself by following two essential practices:

1. Use Masked Aadhaar

Download a **Masked Aadhaar** from UIDAI (myaadhaar.uidai.gov.in). It conceals the first 8 digits (showing `XXXX-XXXX-1234`) while keeping your photo and QR code valid for legal identity verification.

2. Cross-Watermark All Copies

Write a diagonal line across the copy: *"Submitted strictly for recruitment verification at [Company Name] only on [Date]."* This prevents unauthorized use of your document.

WHAT TO DO NEXT (CHAPTER 5 ACTION CHECKLIST)

- ✓ Never enter banking passwords, ATM PINs, or UPI MPINs on any employment form.
- ✓ Never install `.apk` files or remote access apps like AnyDesk or TeamViewer.
- ✓ Only provide identity proofs after verifying the employer and receiving a valid offer letter.
- ✓ Always submit Masked Aadhaar with a clear handwritten purpose watermark.

CHAPTER 6

One-Page Job & Recruiter Verification Checklist

Use this printable audit checklist before applying, paying money, sharing sensitive identity documents, or signing an employment contract. Check each item carefully.

CHECK	VERIFICATION ITEM	VERIFICATION METHOD & STANDARD	YOUR NOTES
☐	Company Identity	Website independently searched; physical office address and MCA CIN registry verified.	
☐	Recruiter Domain	Recruiter emails from corporate domain (`@company.com`), NOT free public webmail (`@gmail.com`).	
☐	Job Description	Role responsibilities, required technical skills, and educational qualifications are clear.	
☐	Salary Benchmark	Compensation is realistic for the industry, not an exaggerated "instant daily payout."	
☐	Official Application	Application submitted via corporate careers portal, ATS link, or established job board.	
☐	Real Evaluation	Underwent structured video/telephonic/in-person interview assessing real competency.	
☐	Zero Fee Demanded	Zero payment demanded for registration, laptop security, uniforms, or training.	
☐	Credential Safety	No bank OTPs, ATM PINs, UPI MPINs, or remote access software (AnyDesk) requested.	
☐	Offer Verification	Offer letter verified independently via official company switchboard or HR email.	

Checklist Scoring Guide

If all 9 boxes are checked: **Proceed Cautiously**. If items 1–3 are ambiguous: **Verify Further**. If item 7 or 8 fails (money demanded or credential requested): **STOP IMMEDIATELY**. This is an active fraud attempt.

The Three-Tier Verification Decision Framework

Use this systematic three-tier decision model whenever you encounter an ambiguous job opportunity or unverified recruiter.

● GREEN TIER PROCEED CAUTIOUSLY

Criteria:

- Corporate domain email confirmed.
- Requisition ID listed on official website.
- Rigorous multistage interview held.
- Salary benchmarks realistic.
- Zero payments requested.

Action: Proceed with onboarding.
Use Masked Aadhaar and watermarked documents.

● YELLOW TIER VERIFY FURTHER

Criteria:

- Contacted via WhatsApp or phone.
- Third-party agency representation.
- New or obscure company website.
- Minor inconsistencies in job role.
- Urgent pressure to accept offer.

Action: Pause. Do not send identity documents. Call central corporate switchboard.

● RED TIER STOP & INVESTIGATE

Criteria:

- Money demanded for any reason.
- Offer issued without an interview.
- Free public email used (`@gmail.com`).
- `.apk` app download requested.
- Demand for bank OTPs or PINs.

Action: Immediately cease all contact. Block the sender, preserve evidence, and report.

FRAMEWORK DISCLAIMER

This decision framework is a practical safety guide designed to eliminate the most common fraud vectors. It is not an absolute guarantee that every opportunity in the Green Tier is genuine, nor that an employer in the Yellow Tier is fraudulent. Always exercise your own critical judgment and independent verification.

HOW TO NAVIGATE BETWEEN TIERS

- ✓ Never move from Yellow to Green without direct, independent confirmation from the hiring company.
- ✓ A single Red flag is enough to stop the process—do not ignore warning signs because you want the job.
- ✓ When in doubt, consult a trusted mentor or career counselor before proceeding.

Real-World Case Studies: Scenarios 1 & 2

Note: All entity and individual names in these illustrative scenarios are completely fictional and presented solely for educational purposes.

Scenario 1: The "Daily Payout" Remote Data Entry Listing

HIGH RISK FRAUD

The Situation: Rahul, a 2nd-year college student, spots an Instagram sponsored post: "Work from Home Data Entry! Earn ₹2,500 daily for typing 20 pages! No experience needed. 100% genuine. WhatsApp HR: 98XXXXXX." Upon messaging, he is approved immediately without a resume check or interview.

Warning Signs: Unrealistic salary (₹75,000/month for basic typing), complete lack of an interview, communication exclusively on WhatsApp, and immediate unearned selection.

What to Verify: Check market compensation for typing services (modest hourly or project fees). Search the MCA registry for the company's legal existence.

Safest Next Step: Disengage immediately and block the number. Never pay the "software registration fee" of ₹1,500 that scammers inevitably demand on day two.

Scenario 2: The Corporate Recruiter Impersonation

DOMAIN SPOOFING

The Situation: Priya, an IT engineer, receives a message on WhatsApp from someone claiming to be "Pooja Sharma, Lead Talent Acquisition at Apex Global Solutions (a reputed IT multinational)." The profile displays the corporate logo, and she receives an email interview invite from `pooja.apexrecruiting@gmail.com`.

Warning Signs: Use of a free public `@gmail.com` address while claiming to represent a multibillion-dollar multinational enterprise.

What to Verify: Visit the authentic corporate portal (`apextech.com/careers`). Search for the real Pooja Sharma on LinkedIn and review her verified company affiliation.

Safest Next Step: Message the real Pooja Sharma directly on LinkedIn or email `careers@apextech.com` to confirm whether the job opening is legitimate.

Real-World Case Studies: Scenarios 3, 4 & 5

Scenario 3: The "Refundable" Laptop Security Deposit

ADVANCE FEE FRAUD

The Situation: Amit clears a brief 10-minute telephonic chat for an "Operations Associate" position with a purported logistics firm. He receives an appointment letter on PDF letterhead offering ₹45,000/month. The HR informs him: *"Your company laptop is ready for courier dispatch. Transfer a refundable deposit of ₹4,999 to our logistics partner UPI handle: logistics-dispatch@paytm."*

Warning Signs: Demand for money via UPI before joining; claiming company-issued hardware requires candidate funding.

Safest Next Step: Amit must refuse payment. He should request official corporate policy from an official domain email. If they insist on payment, immediately cease contact.

Scenario 4: The Part-Time "Task Rating" Scam

RECHARGE SCAM

The Situation: Sneha receives a Telegram message offering a part-time job "reviewing hotels on Google Maps." She writes 3 reviews and receives ₹300 via UPI. Next, she is invited to a "VIP Task Group" where she must transfer ₹3,000 to "unlock high-tier tasks" that promise a ₹5,000 return.

Warning Signs: Small initial payout to build trust, followed by demands for upfront funds to "unlock" higher earning levels.

Safest Next Step: Sneha must exit the Telegram group immediately, block the admins, and report the channel. Never invest money into "task pools."

Scenario 5: The "Salary Account" Phishing Form

PHISHING / CREDENTIAL THEFT

The Situation: Vikram receives an offer letter from a purported software firm. The recruiter sends a link: `https://onboarding-portal-verification.top/bank-details` and instructs him to fill in his details within 24 hours to initiate salary account opening. The form asks for his Name, PAN, Bank Account Number, Internet Banking Username, and Login Password.

Warning Signs: Non-standard web extension (`.top`), unverified third-party URL, and explicit requests for confidential login passwords.

Safest Next Step: Vikram should close the link immediately without typing any information. Clear browser cache, scan his device with antivirus, and report the phishing URL to cyber authorities.

Emergency Response: What to Do if You Suspect Fraud

If you realize you have been scammed, paid money, or shared sensitive documents, **stay calm and act immediately**. Quick action within the first 1 to 2 hours significantly increases the chances of freezing fraudulent transactions.

GOLDEN HOUR ACTION: CALL HELPLINE 1930 IMMEDIATELY

If you transferred money via UPI, net banking, or debit card to a fraudster, call the **National Cyber Crime Helpline: 1930** immediately. Provide your transaction UTR number, bank details, and the fraudster's UPI/account details. Quick reporting allows authorities to freeze the funds in the recipient bank.

Phase 1: Financial Containment

- **Block Banking Cards:** Call your bank's 24×7 helpline or use mobile banking to immediately block compromised debit/credit cards.
- **Change Passwords & MPIN:** Reset your internet banking passwords, UPI MPIN, and email credentials from a different, clean device.
- **Notify Your Bank Branch:** Visit or email your home branch to report the fraudulent transaction and request a dispute chargeback.

Phase 2: Identity Protection

- **Lock Aadhaar Biometrics:** Log in to UIDAI ('myaadhaar.uidai.gov.in') and lock your biometric authentication.
- **Monitor Credit Reports:** Check your CIBIL and Experian credit reports over the next 3 to 6 months for unauthorized loan accounts.
- **Scan Devices for Malware:** If you installed an '.apk' file or software, disconnect from Wi-Fi, uninstall the app, and run a full antivirus scan.

Phase 3: Formal Evidence Preservation & Legal Reporting

Do not delete chat logs or emails out of anger or embarrassment. You will need clear evidence:

- Take timestamped screenshots of the job posting, chat conversations, payment QR codes, and SMS messages.
- Save the transaction reference numbers (UTR, UPI Transaction ID, bank statement entry).
- File a formal cyber complaint on the Government of India portal: '<https://cybercrime.gov.in>'.
- Visit your local Cyber Crime Police Station with printed copies of your evidence.

Official Indian Verification & Reporting Directory

Always rely on official, verified Indian government portals and statutory bodies for reporting cyber incidents and validating corporate credentials.

National Cyber Helpline

Emergency

Dial: 1930 (Toll-Free, 24x7)

Immediate citizen reporting helpline for financial cyber fraud, managed by the Indian Cyber Crime Coordination Centre (I4C).

Cyber Crime Portal

Filing

<https://cybercrime.gov.in>

Official Government of India portal to register formal cybercrime complaints and upload evidence.

Ministry of Corporate Affairs

Registry

<https://www.mca.gov.in>

Verify legitimate company existence, CIN numbers, registered office addresses, and director details.

National Career Service

Verified Jobs

<https://www.ncs.gov.in>

Ministry of Labour and Employment initiative providing authentic job listings and career centers.

UIDAI Aadhaar Portal

Identity

<https://myaadhaar.uidai.gov.in>

Download official Masked Aadhaar copies and lock biometric access to prevent unauthorized misuse.

Chakshu (Sanchar Saathi)

Telecom

<https://sancharsaathi.gov.in>

Department of Telecommunications portal to report fraudulent calls, SMS, and WhatsApp communications.

OFFICIAL DISCLAIMER & TERMS OF USE

This handbook is published as part of the **Job Seeker Success Kit** to provide general educational guidance and fraud awareness for job seekers across India. The methodologies, warning signs, and verification steps represent industry best practices in cybersecurity and recruitment ethics. However, cybercrime tactics evolve continuously, and this guide does not constitute legal or financial advice. We cannot guarantee that any prospective employer is genuine or fraudulent. Readers must conduct independent verification and consult official law enforcement authorities in active criminal cases.