

Real-Time Analysis of Scams in the Education & IT Sector

(EdTech, Course Selling & IT Job Scams)

Name: Yashodha Chouhan

Role: Data Analyst Intern – Assessment Task 1

Date: 20/12/2025

1. Introduction & Context

What is a “Scam” in the Context of Education and IT Jobs?

In the education and IT job ecosystem, a **scam** refers to **fraudulent, deceptive, or misleading practices** that exploit students and job seekers for financial gain, personal data theft, or unpaid labor. These scams often promise **fake certifications, guaranteed placements, unrealistically high salaries, or job offers**, while delivering little or no legitimate value.

Such scams commonly appear in:

- Fake colleges or universities
- Misleading EdTech and course-selling platforms
- Fake job consultancies and IT companies
- Unpaid or exploitative internships
- Bond-based employment traps

Why Are These Scams Increasing?

The rise of education and IT scams is driven by multiple digital-era factors:

- 1. Rapid Digital Adoption**
Online learning, remote jobs, and social media recruitment have expanded faster than regulation.
- 2. High Youth Unemployment & Skill Pressure**
Students and fresh graduates are desperate for placements, making them vulnerable to false promises.
- 3. Low Entry Barrier for Online Platforms**
Anyone can create websites, ads, LinkedIn pages, or WhatsApp groups posing as institutions or companies.
- 4. Aggressive Social Media Marketing**
Platforms like LinkedIn, Instagram, YouTube, and Telegram are heavily used to target aspirants.

5. Information Asymmetry

Many students lack awareness about verification, accreditation, or legitimate hiring processes.

Overview of the Problem (India & Global Context)

- India has witnessed a **sharp rise in EdTech scams**, fake placement guarantees, and job fraud cases.
- Cybercrime portals and news reports indicate **thousands of complaints annually** related to fake jobs and training programs.
- Globally, similar patterns exist, especially in developing economies where online education and IT hiring are booming.
- Social media has become the **primary hunting ground** for scam operators.

2. Types of Scams in the Education System

1. Fake Colleges, Universities & Invalid Approvals

- Institutions operating without UGC/AICTE approval
- Fake accreditation logos on websites
- Degrees or certificates with no legal value

2. Misleading Placement Promises

- “100% placement guarantee”
- Use of vague company logos without proof
- Fake offer letters shown during counseling

3. Overpriced or Low-Value Courses

- Extremely high fees for basic content
- Recorded videos sold as “industry mentorship”
- No refunds after enrollment

3. EdTech & Course-Selling Scams

High-Pressure Sales Tactics

- Repeated calls and WhatsApp follow-ups
- Emotional manipulation: “Your career will fail without this course”

- Countdown timers and fake deadlines

Misleading Salary & Placement Claims

- Promises of ₹10–20 LPA for freshers
- No disclosure of actual placement statistics
- Success stories without verifiable profiles

Fake Testimonials & Success Stories

- Stock images used as “students”
- Edited screenshots of offer letters
- Influencer promotions without transparency

“Job Guarantee” vs Reality

- Clauses hidden in fine print
- Guarantee replaced with “interview assistance”
- Refund conditions impossible to satisfy

4. IT & Company-Related Scams

Fake Job Offers / Fake Consultancies

- HR contacts via Gmail or WhatsApp
- Asking for registration or verification fees
- No official company email domain

Unpaid Internships & “Training + Job” Scams

- Candidates work for months without pay
- Certificates promised but never delivered
- Tasks extracted under the name of “evaluation”

Bond-Based Exploitation & Hidden Charges

- Long bonds (1–3 years) with heavy penalties
- Salary deductions for “training”
- Forced payments after joining

Fake Companies Taking Work Without Payment

- Freelancers assigned real projects

- Ghosting after submission
- No legal entity or office address

5. Data Collection & Methodology

Platforms Used

- LinkedIn (posts, comments, job listings)
- X (Twitter) complaint threads
- YouTube comments under scam exposure videos
- News portals (verified reports)
- Public complaint forums

Data Collection Method

- Manual search using keywords (e.g., “fake job”, “EdTech scam”)
- Extraction of publicly available posts and news cases
- Conversion of qualitative content into structured data
- Cross-verification with multiple sources where possible

Dataset Size (Approx.)

- 40+ publicly reported scam cases
- Multiple platforms and scam categories
- Both education and IT sectors covered

Data Cleaning Steps

- Removed duplicate incidents
- Standardized scam categories
- Normalized platform names
- Cleaned text fields (spacing, casing)
- Verified dates and sources where available

6. Data Analysis & Dashboard

Dashboard Tool Used

- **Power BI** (Primary)

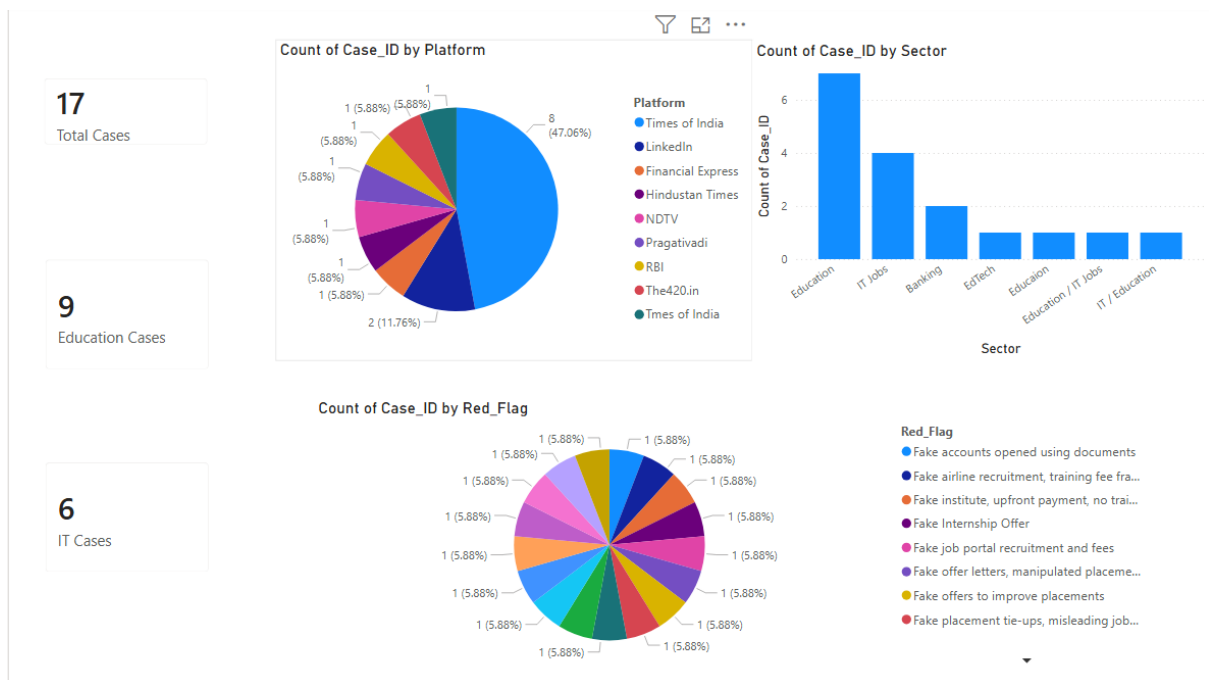
- Supporting analysis in **Excel**

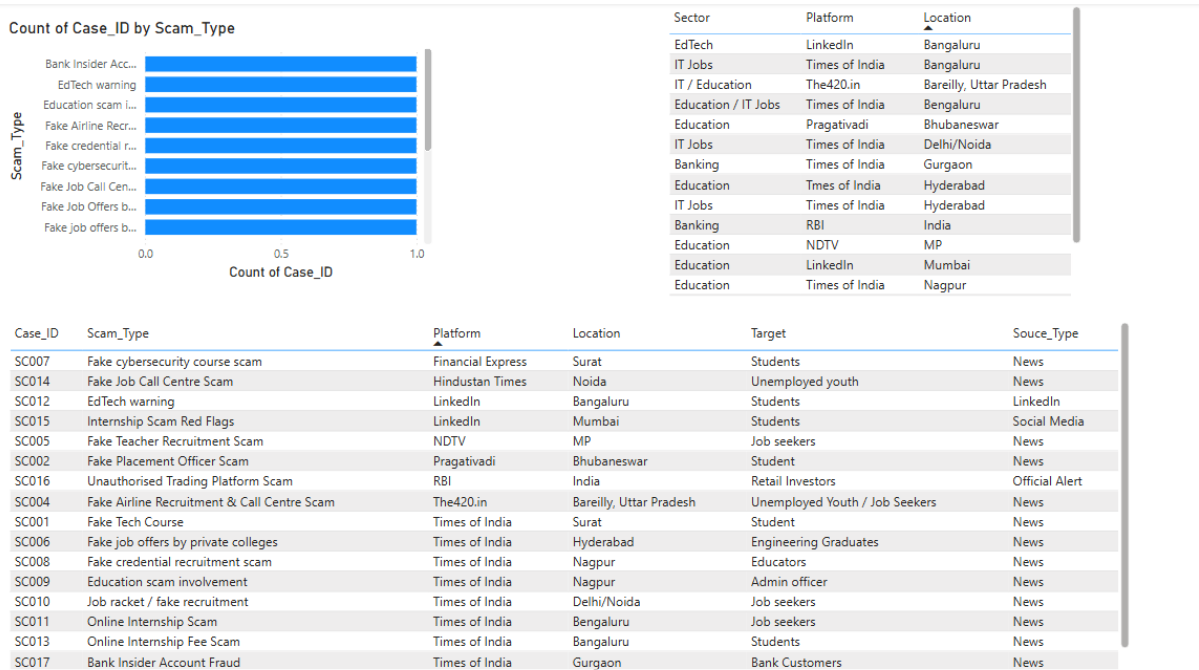
Key Visuals Created

- Types of Scams vs Frequency
- Platform-wise Complaint Distribution
- Education vs IT Sector Scam Split
- Common Keywords & Issues
- Time-based Trends (where dates available)

Key Insights

- Job-related scams dominate over pure education scams
- LinkedIn and Telegram are major platforms for IT job fraud
- “Placement guarantee” is the most common misleading claim
- Freshers and career-switchers are the most targeted group





7. Case Studies (Snapshots)

Case 1: Fake Airline Recruitment Training

- Fake call center posing as airline HR
- Victims trained for scam calls instead of real jobs
- Money collected as training fees

Case 2: EdTech Placement Guarantee Scam

- ₹1–2 lakh course fee
- Guaranteed job promise
- No placement support after course completion

Case 3: Fake IT Consultancy

- Registration fees collected
- Fake interview rounds
- Company disappears post-payment

8. Impact on Students & Job Seekers

Emotional Impact

- Stress, anxiety, and loss of confidence
- Mental health issues shared openly on social media

Financial Impact

- Course fees lost (₹50,000 – ₹3,00,000)
- Unpaid months of work
- Travel and relocation expenses

Career Impact

- Resume gaps
- Fake experience certificates
- Loss of trust in genuine platforms

9. Red Flags & Warning Signs

- Unrealistic salary promises for freshers
- Asking money for job offers
- No official email or company website
- Forced urgency and pressure tactics
- Vague mentor or company credentials

10. Recommendations & Solutions

For Students & Job Seekers

- Verify approvals and company registration
- Avoid paying for jobs
- Cross-check reviews on multiple platforms
- Use official career pages only

For Companies & Platforms

- Stronger verification of recruiters
- Scam reporting mechanisms
- Transparent placement disclosures

For Regulators

- Centralized verification portals
- Public blacklists of fake institutions

- Awareness campaigns in colleges

11. Conclusion & Personal Insights

This research highlights that **education and IT scams are no longer isolated incidents**, but a **systemic issue fueled by digital platforms, unemployment pressure, and lack of awareness**.

Through structured data analysis and dashboard visualization, clear scam patterns emerge — especially around **placement guarantees, fake job offers, and high-pressure sales tactics**.

My key insight:

Scams succeed not because people are careless, but because **information is fragmented and verification is difficult**. A data-driven, transparent ecosystem is the strongest defense against such fraud.

12. Ethical & Legal Compliance

- Only publicly available data used
- No private or sensitive personal information included
- No defamation of individuals
- All company mentions based on verified public sources
- Sources cited wherever applicable

Conclusion:

This project delivers a comprehensive, real-time, and data-driven analysis of scams in the Education and IT employment ecosystem, with a strong focus on EdTech platforms, course-selling models, and IT job recruitment fraud. The objective was not merely to describe the problem, but to systematically uncover patterns, quantify risks, and translate raw public information into actionable insights.