

EDUCATION AND IT SECTOR SCAMS REPORT

Domain: Data Analytics

This report is prepared as part of the internship program and focuses on identifying scams in the education and IT sectors. The study analyzes real-world cases, their effects, and the role of technology and awareness in preventing such scams.

Department of Computer Applications
Raj Kumar Goel Institute of Technology

Submitted by.

Name : Swastika Rai.

Submitted To

Name : Mr. Vaibhav Jamre

INTRODUCTION

With the rapid expansion of digital technologies, online education platforms, and IT-based employment opportunities, incidents of fraud and scams in the education and IT sectors have increased significantly. Students, freshers, job seekers, and working professionals are increasingly targeted through fake admissions, fraudulent online courses, counterfeit certifications, and deceptive job offers. These scams often exploit the lack of awareness, urgency for career growth, and trust in digital platforms.

Education and IT sector scams not only result in substantial financial losses but also cause long-term psychological stress, career delays, and loss of confidence among victims. The widespread use of messaging applications, unverified websites, and unauthorized agents has further enabled scammers to operate at scale with minimal accountability.

This report presents a real-time inspired data analysis of education and IT sector scams in India using a structured dataset derived from publicly reported cases and observed scam patterns. The analysis aims to identify common scam types, platforms used, vulnerable target groups and financial impact. By examining these patterns, the study provides actionable insights and recommendations to enhance awareness, improve verification mechanisms and reduce the occurrence of such scams in the digital ecosystems.

Objectives of the study

The objectives of this study are as follows:

1. To analyze the occurrence of scams in the education and IT sectors.
2. To identify the most common types of scams affecting students and job seekers.
3. To examine the platforms frequently used by scammers to execute fraudulent activities.
4. To understand the target groups most vulnerable to education and IT sector scams.
5. To assess the financial impact of these scams based on reported and observed data.
6. To identify common red flags and scam patterns used by fraudsters.
7. To provide data-driven insights and recommendations to reduce scam risks and improve awareness.

Scope of the Study

The scope of this study is limited to the analysis of scams occurring in the education and IT sectors in India. The study focuses on fraudulent activities such as fake admissions, online course scams, scholarship frauds, fake job offers, overseas job scams, and fraudulent internships.

The analysis covers scam cases reported or observed between 2023 and 2025, targeting students, freshers, job seekers, working professionals, parents, and freelancers. The dataset used in this study is pattern-based and inspired by real-world cases reported through news articles, cybercrime portals, and public complaint platforms.

This study aims to identify trends, patterns, and insights related to scam execution methods, platforms used, and financial impact, without investigating individual legal cases.

Data Sources

The dataset used for this analysis was compiled using information from the following sources:

1. Online news articles reporting education and IT sector scams
2. Cybercrime awareness and reporting portals
3. Consumer complaint forums and public grievance websites
4. Blogs, case studies, and publicly available reports on digital fraud

Due to confidentiality and limited availability of detailed public records, certain data values such as exact financial losses were estimated or marked as indicative. These assumptions have been made solely for analytical and educational purposes.

Methodology

The methodology adopted for this study consists of the following steps:

1. Identification of common scam cases related to the education and IT sectors.
2. Collection and categorization of scam information based on sector, scam type, platform used, target group, and financial loss.
3. Creation of a structured dataset using Microsoft Excel.
4. Data cleaning by handling missing values, standardizing categories, and ensuring data consistency.
5. Exploratory data analysis using pivot tables and summary statistics.
6. Visualization of key trends through charts and graphs.
7. Interpretation of results to generate insights and actionable recommendations.

This structured approach ensures systematic analysis and meaningful interpretation of scam patterns.

Dataset Overview

The dataset consists of 50 records of education and IT sector scams in India between 2023 and 2025. Each record represents a single scam case with the following attributes:

1. Scam_ID – Unique identifier for each case
2. Sector – Education or IT
3. Scam_Type – Type of scam (e.g., fake job, fake course, scholarship fraud)
4. Platform_Used – Medium used by scammers (WhatsApp, Telegram, website, email, agent)
5. Target_Group – Victim group (students, freshers, job seekers, parents)
6. Amount_Lost_INR – Financial loss in Indian Rupees
7. Location – Indian state where victims are located
8. Year – Year of reported scam

9.Key_Promise – The lure offered by scammers (job, admission, degree, scholarship)

10.Red_Flag – Warning signs of fraud (upfront fees, fake documents, urgent deadlines)

Data Analysis and Finding

The analysis of the 50-record dataset reveals key patterns in education and IT sector scams:

1. Sector-wise Scam Distribution

IT Sector: 26 cases (52%) – mostly fake job offers, overseas job scams, and fraudulent internships.

Education Sector: 24 cases (48%) – mainly fake admissions, online courses, scholarships, and degree fraud.

2. Common Scam Types

Education Scams: Fake admissions, online courses, scholarships, fake degrees.

IT Scams: Fake jobs, overseas job promises, fake internships, remote/freelance jobs.

3. Platforms Used

WhatsApp & Telegram – 60% of scams

Email & Websites – 25%

Agents/Consultancies – 15%

4. Target Groups

Students – 40%

Freshers/Job Seekers – 50%

Parents/Professionals/Freelancers – 10%

5. Financial impact

Education scams: INR 3,000 – 5,00,000 (mostly small but frequent losses)

IT scams: INR 15,000 – 7,20,000 (large financial impact per case)

6. Red Flags Observed

Requests for upfront fees or deposits
Fake offer letters, degrees, or certificates

Urgent joining deadlines

No official verification or communication channels

7. Trends Over Time (2023–2025)

Scam frequency is increasing slightly each year, especially IT-related overseas job scams.

Education scams remain consistent, mostly smaller in monetary value but widespread

Key Insights

Over 60% of scams occur through messaging platforms like WhatsApp and Telegram

Freshers and students are the most vulnerable groups across both sectors.

IT overseas job scams result in the highest financial losses per case.

Red flags such as upfront fees, fake offer letters, and urgent joining deadlines are common in most scams.

Education scams exploit trust in online learning platforms, fake degrees, and scholarship schemes.

Scam frequency shows a slight increasing trend over 2023–2025, especially in the IT sector.

Recommendations

Conduct awareness programs in colleges, universities, and job training centers.

Ensure verification of recruitment agencies, education platforms, and agents before engagement.

Promote official government portals for admissions, scholarships, and job postings.

Train students and job seekers in digital literacy, highlighting common red flags.

Strengthen reporting mechanisms and quick action by cybercrime authorities.

Encourage victims to report scams immediately to prevent further incidents.

Limitations of the Study

The dataset is pattern-based and does not include all real-world cases.

Some financial values are estimated due to limited public information.

Geographic coverage is limited to reported cases and may not represent every state.

The analysis is observational, without legal investigation or validation of individual cases.

Conclusion

Education and IT sector scams are increasingly prevalent in the digital era. The analysis highlights critical trends in scam types, target groups, platforms used, and financial impact. IT scams, particularly overseas job frauds, cause the largest losses, while education scams exploit trust and urgency among students.

By understanding these patterns and implementing preventive measures such as awareness campaigns, verification of platforms and agents, and reporting mechanisms, both students and job seekers can be better protected. A data-driven approach is essential to reduce fraud and ensure a safer digital environment for education and employment opportunities.