



Job Guard

Brought to you by Katherine Barrios, Andrea Matos, Genaro Brito, Michal Rodney and Obilio Cardozo



What's the Problem?

- In a statistic shared by the Labor Department to the *Wall Street Journal*, “More than 1.6 million of the 7 million Americans unemployed as of last November had been job hunting for at least six months.”
- The availability of entry level jobs is declining, putting recent grads and career transitioners at a disadvantage
- Despite all of this, job boards and sites have a growing rotation of listings
- Greenhouse (a hiring platform) discovered, in a recent study, that 18-22% of the listings on the site were fraudulent





What Constitutes a Fraudulent Listing?

A fraudulent listing is designed to sell a user an opportunity to apply to a job that never existed. This could be for many reasons, like:

- Stealing information
- Granting access to an applicants bank information
- Tricking applicants into participating in illegal activities

With these listings, there was never an intention to hire a candidate, only to pique their interest for long enough to collect sensitive information.





Red Flags to Look Out For

- Too Good to be True
- Vague or Missing Information
- Pressure Tactics
- Requests for Personal or Financial Information
- Unusual Communication Methods
- Suspicious Application Process



Our Solution



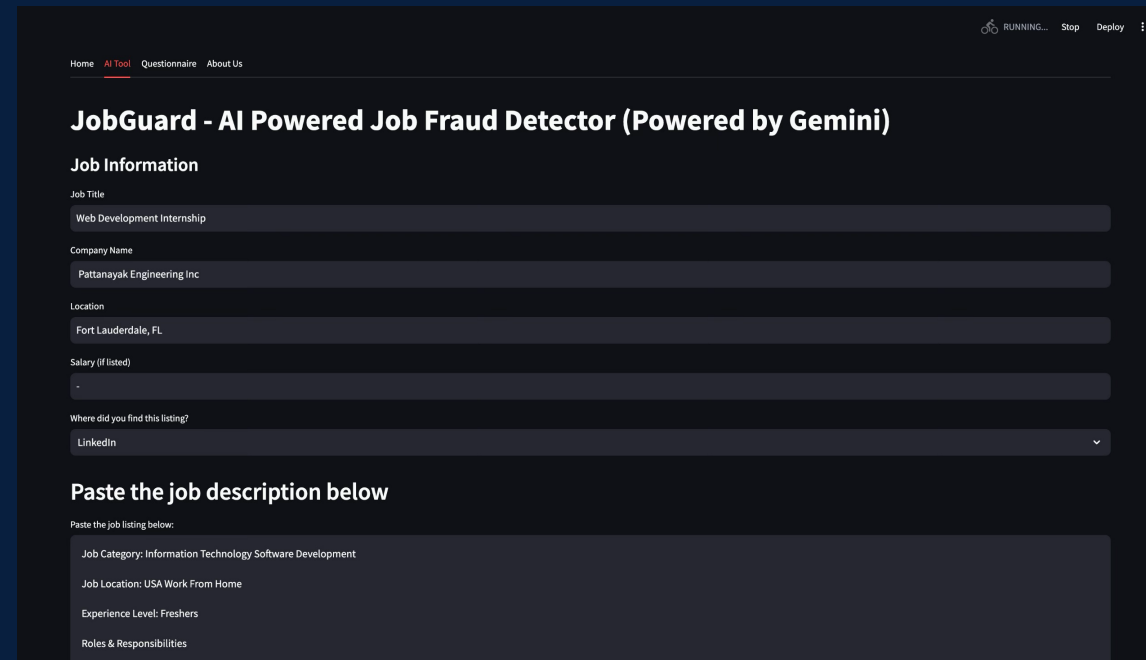
FIU

Engineering
& Computing

FLORIDA INTERNATIONAL UNIVERSITY

What Does JobGuard Do?

Step One



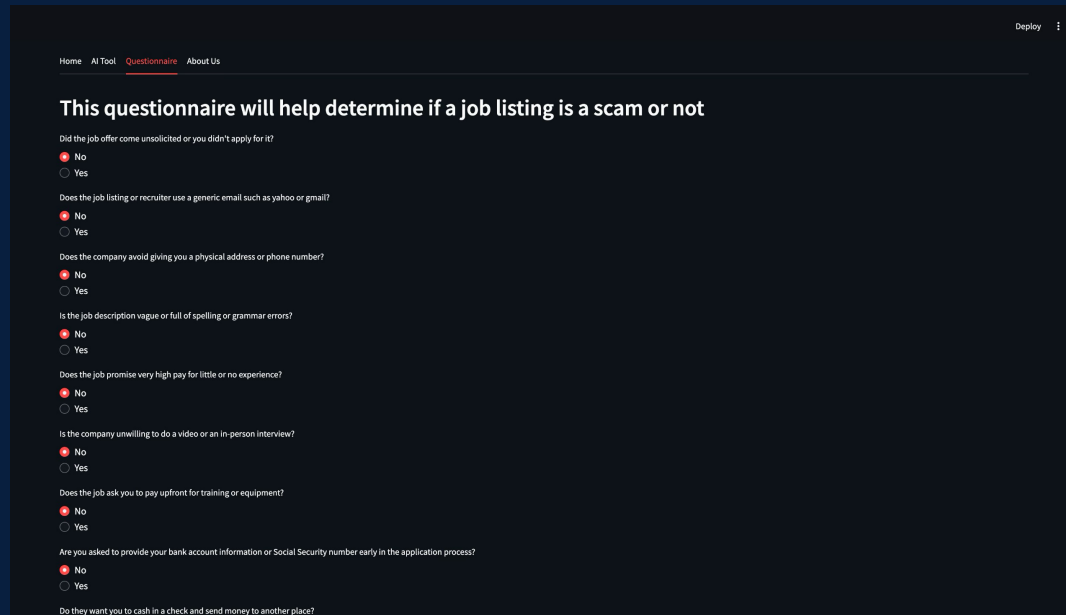
The screenshot shows the JobGuard web application interface. At the top, there is a navigation bar with links for Home, AI Tool, Questionnaire, and About Us. The main heading is "JobGuard - AI Powered Job Fraud Detector (Powered by Gemini)". Below this, the "Job Information" section contains several input fields: "Job Title" (filled with "Web Development Internship"), "Company Name" (filled with "Pattanyak Engineering Inc"), "Location" (filled with "Fort Lauderdale, FL"), "Salary (if listed)" (filled with "-"), and "Where did you find this listing?" (a dropdown menu filled with "LinkedIn"). Below the input fields, there is a section titled "Paste the job description below" with a text area containing the following text: "Job Category: Information Technology Software Development", "Job Location: USA Work From Home", "Experience Level: Freshers", and "Roles & Responsibilities".

JobGuard allows a user to input information from a listing they might be questioning as fraudulent



What Does JobGuard Do?

Step Two



The screenshot shows a web application interface for a questionnaire. At the top, there is a navigation bar with links for 'Home', 'AI Tool', 'Questionnaire' (which is highlighted), and 'About Us'. A 'Deploy' button is visible in the top right corner. The main heading reads 'This questionnaire will help determine if a job listing is a scam or not'. Below this, there are ten questions, each with a red radio button next to 'No' and a grey radio button next to 'Yes'. All 'No' options are selected. The questions are:

- Did the job offer come unsolicited or you didn't apply for it?
- Does the job listing or recruiter use a generic email such as yahoo or gmail?
- Does the company avoid giving you a physical address or phone number?
- Is the job description vague or full of spelling or grammar errors?
- Does the job promise very high pay for little or no experience?
- Is the company unwilling to do a video or an in-person interview?
- Does the job ask you to pay upfront for training or equipment?
- Are you asked to provide your bank account information or Social Security number early in the application process?
- Do they want you to cash in a check and send money to another place?

JobGuard will then ask the user some basic questions to help the algorithm determine if a listing is fraudulent





What Does JobGuard Do?

Step Three

Deploy

Analyze Listing

Analysis Complete.

Based on the analysis of the provided job listing, here is the evaluation:

- Verdict: Fraudulent
- Confidence: 95%
- Margin of error: 5%
- Conclusion and explanation:

This job listing carries multiple, significant red flags that strongly indicate it is fraudulent. While it may not be a traditional scam aimed at stealing money, it qualifies as fraudulent because it is highly deceptive, likely illegal, and not a genuine job opportunity.

Here is a breakdown of the evidence:

Major Red Flags:

1. **Expired Job Posting:** The most conclusive piece of evidence is the start date: "between 31st Jul'20 and 4th Sep'20". This listing is for an internship that was supposed to start four years ago. This indicates it is either a "ghost job" posted to collect resumes and data, or a scammer is lazily reusing old text without updating it. In either case, it is not a current, real opportunity.
2. **Unpaid Internship (No Salary):** The salary is listed as "-". The "Perks & Other Benefits" section lists only a certificate and a letter of recommendation, which are common offerings used to justify not paying interns. For a for-profit company in the US like "Pattasayan Engineering Inc.", unpaid internships are subject to strict legal tests (the 7-point primary benefit/carry test from the Department of Labor). The responsibilities listed, such as "maintaining hosting and updates of websites" and building out a base theme, sound like work that a regular employee would do. This strongly suggests the internship would not be legal, as it appears to benefit the employer more than the intern.
3. **Vague and Grandiose Company Description:** The "About Us" section is filled with high-level buzzwords like "AI, IoT, Space Tech, AR and VR." However, the actual job is a very basic WordPress development role. This disconnect is a common tactic used by small or non-existent companies to appear more impressive and established than they are.
4. **Uncommon Terminology:** The use of the term "Freshers" is much more common in South Asian job markets (like India) than in the United States. While not a definitive red flag on its own, its presence in a US-based listing is unusual and suggests the text may have been copied from another source or written by someone unfamiliar with US hiring norms.

Minor Legitimate Elements (That Don't Outweigh the Red Flags):

- **Plausible Job Duties:** The technical responsibilities (WordPress, HTML/CSS, Mailchimp) are standard and appropriate for a web development internship.
- **Company Website:** The inclusion of a URL lends a thin veil of legitimacy. However, the existence of a website is easy to fake and does not verify the legitimacy of the job offer itself.

Conclusion:

The job listing is fraudulent. It advertises a position that is years out of date. Furthermore, it describes an unpaid role at a for-profit company that involves substantive work, making it highly exploitative and almost certainly illegal under US labor law. The combination of these factors makes it clear that this is not a legitimate opportunity for a job seeker. It is either a data-harvesting "ghost job" or a template for a labor exploitation scam.

Conclusion:

The job listing is fraudulent. It advertises a position that is years out of date. Furthermore, it describes an unpaid role at a for-profit company that involves substantive work, making it highly exploitative and almost certainly illegal under US labor law. The combination of these factors makes it clear that this is not a legitimate opportunity for a job seeker. It is either a data-harvesting "ghost job" or a template for a labor exploitation scam.

AI Verdict Visualization

Confidence Score Verdict: Unknown

0
▼-100

Downloads

Download TXT Download PDF Download CSV



JobGuard will then provide a report outlining the red (or green) flags found in the listing and rank the listing with a Confidence Verdict



What Does JobGuard Do?

Step Four (Optional)

Excellent. Let's analyze this job listing for fraudulent activity.

Analysis of Job Listing

Verdict: Fraudulent

Confidence: 95%

Margin of error: 5%

Conclusion and explanation:

This job listing exhibits multiple, significant red flags that strongly indicate it is a fraudulent "internship mill" scam rather than a legitimate employment opportunity. The goal of such scams is typically to acquire free labor for menial tasks, sell worthless "training" or "certificates," or simply build a facade of a real company.

Here is a breakdown of the evidence:

1. **Outdated and Recycled Content:** The most glaring red flag is the date range: "can start the work from home job/internship between **31st Jul/20 and 4th Sep/20**". This is a listing from 2020. A legitimate company would not be actively recruiting for a position that started years ago. This indicates a copy-pasted, recycled scam template that the operators did not bother to update.

2. **Implied Unpaid Labor for a Skilled Role:** The listing conspicuously omits any mention of salary or compensation. Instead, it offers "perks" like a "Certification" and a "Letter of recommendation." Legitimate .NET development internships in the US are almost universally paid, as they require valuable technical skills. Offering non-monetary, low-cost perks in place of a salary is a classic tactic of exploitative internship mills. The "certification" is likely a self-issued, worthless document.

3. **Vague and Generic Responsibilities:** The roles are extremely vague: "Understanding and developing .net projects" and "Learn and upgrade." A real job description would specify the types of projects, the technologies involved (beyond just ".NET"), and the team structure. The addition of "Perform customer engagement role" is unusual and out of place for a development intern, suggesting tasks may be unrelated to actual software development (e.g., cold calling, data entry).

4. **Cultural/Linguistic Red Flags:** The use of the term ""Freshers"" to mean "entry-level" or "recent graduates" is not standard in American English for job postings. It is, however, extremely common in India. This, combined with a US-based company, suggests the listing was written by someone outside the US or is targeting applicants from that region, which is a common pattern for certain types of online scams.

5. **Grandiose and Unverifiable Claims:** The company description is filled with buzzwords ("AI, IoT, Space Tech, AR and VR") that sound impressive but are wildly inconsistent with a company offering a single, vague, unpaid internship. It is highly improbable that a small company headquartered in Weston, FL, is a major player in "Space Tech" while simultaneously being unable to pay a development intern.

The Likely Scam:

This is a textbook example of an "internship mill". The business model is to attract a large number of students or recent graduates with the promise of "experience." The "interns" are then given menial, non-educational tasks that provide free labor for the company. At the end of the "internship," they may be pressured into paying a fee for the promised "certification," which is the ultimate goal of the scam. The experience gained is rarely valuable or relevant.

Recommendation: Avoid this listing and any similar offers. Always be suspicious of technical internships that are unpaid, have vague job descriptions, and make claims that seem too good to be true.





Why Is This Helpful?

- We hope to bring some ease to the job hunting process for students and young professionals like ourselves
- We hope to minimize the amount of job hunters who, after countless attempts at finding work, let their guard down enough to engage with fraudulent listings
- We hope to help job hunters maximize their time and focus on listings that have high confidence scores and will have greater chances of getting hired legitimately





Future Features

- User profiles —> Any user can create their own account and save listings to their profile
- Scammy Company Database —> A collection of companies that have commonly been added to the site by users that have frequently posted fraudulent job listings
- Chrome Extension —> An extension for Google Chrome that could scrape a job board of the user's choice and return a report of the listings in question





Thank You for Your Time!



Engineering
& Computing

FLORIDA INTERNATIONAL UNIVERSITY