

How Are Security Job Postings Screening and Authenticating Candidates? Scam Warnings Rose, and a Few Employers Now Name Identity Checks

AKA Security Research Factory^{*}

AKA Security

akasecurity.io/research/candidate-screening-and-authentication

1 October 2026

AKA-RZ:2610.10v1 · Version 1.0.0

Abstract

US security job postings, 2024 against 2026: recruiting-scam and impersonation warnings went from 0.7% to 11.3%. A few employers now name identity checks.

^{*}Written entirely by agents in the Research Factory, within guardrails and controls set by our team. Figures as of 1 October 2026.

1 Introduction

A posting shows only what an employer chose to write down. Read that way, 2.5% of 2026 security postings at US-headquartered companies name a candidate identity check or a camera-on or in-person interview or onboarding requirement. None of 1,038 US postings in spring 2024 did. The rise is likely but borderline, and two employers, General Dynamics Information Technology and Cloudflare, account for 54% of the postings that name one.

Warnings about recruiting scams and impersonation moved further, from 0.7% of postings to 11.3%, a change of +10.6 points (likely range +7.1 to +14.5). These work in the other direction: the employer warns candidates about scams and people posing as its recruiters. This read covers security job postings only. A version across all jobs will follow once the collection covers every job description. Background checks are named about as often as in 2024. Candidate-fraud screening, from fraud-detection tools to bans on AI tools in interviews, appears in 2.0% of 2026 postings, again a likely but borderline rise.

2 The answer at a glance

Table 1: Findings with their confidence and representativeness ratings, on the scales defined in [1].

Finding	Confidence	Representativeness
Postings naming an identity check or a camera-on or in-person interview or onboarding requirement rose from 0.0% to 2.5%, a likely but borderline rise	Medium. A likely but borderline rise (likely range +0.8 to +4.8). Among companies with postings in both years there is no clear change (+0.0 to +15.9), so the rise is not shown to hold there.	Low. 18 employers, and two of them carry 54% of the 115 postings.
Background checks are named in 4.6% of 2024 postings and 6.2% of 2026 postings, with no measurable change	Medium. The likely range, -1.4 to +4.7 percentage points, stays within 5 points of zero, but not in every check. Counted once per employer, the rate shows a likely but borderline rise (+0.3 to +5.4). Compared only with 2024 postings applied through a company job board, the range reaches down to -6.3.	Medium. 37 employers in 2024 and 69 in 2026.
Candidate-fraud screening and interview-integrity rules rose from 0.1% to 2.0%, a likely but borderline rise	Medium. A likely but borderline rise (+0.5 to +3.9). Among postings of similar length there is no clear change (-0.4 to +1.5), so the rise is not shown to hold there.	Low. 12 employers, and two of them carry 53%.
Recruiting-scam and impersonation warnings rose from 0.7% to 11.3%	High. A clear rise, and it stays clear in every check. Among companies with postings in both years, the rise is likely but borderline (+1.0 to +20.7).	Medium. 81 employers. The 2024 and 2026 collections kept different amounts of each posting's closing text.

3 The numbers

Table 2: The numbers.

Measure	Postings with it, 2024 → 2026	2024	2026	Change, points	Likely range (95%)	Employers, 2026
Identity check, or camera-on or in-person interview or onboarding	0 → 115	0.0%	2.5%	+2.5	 +0.8 to +4.8	18
Identity verification step	0 → 64	0.0%	1.4%	+1.4	 +0.3 to +3.3	11
Camera-on or in-person interview or onboarding	0 → 104	0.0%	2.3%	+2.3	 +0.6 to +4.5	13
Background check named	48 → 284	4.6%	6.2%	+1.6	 -1.4 to +4.7	69
Candidate-fraud screening or interview-integrity rule	1 → 90	0.1%	2.0%	+1.9	 +0.5 to +3.9	12
Recruiting-scam or impersonation warning	7 → 517	0.7%	11.3%	+10.6	 +7.1 to +14.5	81
E-Verify or I-9 eligibility line	18 → 192	1.7%	4.2%	+2.5	 +0.2 to +5.0	33

Source: AKA Security analysis. 2024: 1,038 US postings from a public LinkedIn dataset (5 to 19 April 2024). 2026: 4,587 postings at US-headquartered companies in AKA's job-board data. Both years are counted the same way. Likely ranges (95%) are in percentage points, estimated by resampling whole companies rather than single postings. A change in bold is a clear rise. The first three rows, fraud screening and the eligibility line are likely but borderline rises, and the background check is not measurable. A posting can carry several measures.

Bars show each range of likely values against zero (dashed). Solid: the whole range is above or below zero. Grey: it ends at zero. Hollow: it includes zero.

4 Identity checks and camera-on interviews

Two kinds of language count here. The first is a step that checks who the candidate is. General Dynamics Information Technology writes: "As part of the hiring process, we will ask you to complete an identity verification process that leverages advanced biometrics and artificial intelligence to ensure authenticity and protect against identity fraud." Allstate asks: "Please also have a Valid Photo Identification available at the start of your interview."

The second is a requirement that the candidate be seen. Figma writes: "To ensure the integrity of our hiring process and facilitate a more personal connection, we require all candidates keep their cameras on during video interviews." Cloudflare tells applicants at the offer stage that they "may be asked to attend an in-person interview within one of the Cloudflare Offices or Cloudflare Hubs."

General Dynamics Information Technology and Cloudflare carry 62 of the 115 postings, 54%. Without them, 1.2% of 2026 postings name a step, still a likely but borderline rise (+0.5 to +2.1). Counted once per employer, 2.2% of employers name one, a clear rise (+1.2 to +3.1). The 2024 figure stays at zero among the 131 postings applied to through a company job board. Their text kept the equal-opportunity statement, a common closing line, 67.2% of the time.

5 Background checks and fraud screening

Background checks were already named in 2024 postings, and the rate did not measurably move: 4.6% of postings in 2024, 6.2% in 2026 (−1.4 to +4.7). OpenAI and Arctic Wolf carry 21% of the 2026 mentions. Security clearance investigations count here.

Fraud-screening language is rarer, and almost absent from the 2024 postings. Samsara names "a fraud detection tool, to validate the authenticity of applications and protect against identity fraud." Marvell bars AI tools in interviews, and Micron Technology warns that misrepresented qualifications disqualify a candidate. Together these reach 2.0% of 2026 postings, and General Dynamics Information Technology and Micron Technology carry 53% of them.

6 Recruiting-scam and impersonation warnings

These warnings sit in the closing text of a posting. Hewlett Packard Enterprise writes: "We have become aware of an increase in fraudulent recruitment activities in which individuals impersonate our company or authorized recruitment agencies to offer fake employment opportunities." Most name the only email domain recruiters use, or state that the company never asks candidates for money.

The warning appears in 11.3% of 2026 postings from 81 employers. Anthropic and Anduril Industries carry 15% of the 517.

Table 3: Recruiting-scam and impersonation warnings.

Source	Postings	Scam or impersonation warning	Equal-opportunity statement
2024, applied through a company job board	131	2.3%	67.2%
2024, other LinkedIn postings	907	0.4%	35.1%
2026, Workday	1,732	14.8%	68.2%
2026, Greenhouse	1,161	15.6%	60.5%
2026, Ashby	553	7.4%	50.6%
2026, Lever	224	0.0%	0.4%
2026, other boards	917	4.3%	34.7%

Source: AKA Security analysis. The equal-opportunity statement is a closing line most employers carry, used here to see whether closing text survived collection.

The source matters in both years. LinkedIn postings not applied through a company job board keep the equal-opportunity statement about half as often, so the 2024 rate may undercount warnings. Set against the board-applied 2024 postings alone, all 2026 postings, which come from company job boards, still show a rise in the warning from 2.3% to 11.3% (+3.9 to +13.8). In 2026, Lever postings in this data carry almost no closing text, and their 0.0% may undercount the other way.

The same employers point the same direction. At the companies with postings in both years, the warning went from 3.6% of their 2024 postings to 13.7% of their 2026 postings, a likely but borderline rise (+1.0 to +20.7).

7 Where the data comes from

The 2024 postings come from the LinkedIn Job Postings dataset (Hugging Face `datastax/linkedin-job-listings` [2]): 1,038 US postings from 679 companies. The 2026 postings come from AKA's daily read of company job boards: 4,587 security postings from 831 US-headquartered companies, open on or after 23 September 2026. Before 21 September the collector skipped several non-engineering titles, so postings that closed earlier are left out. Postings by job aggregators, which are not employers, are left out in both years. Both years hold the posting text each collection kept.

Both years are counted the same way. A posting counts when its title passes the series' security title rules, a local model reads the posting and judges it a security role, and it is the only posting with that title at that company.

Each measure is a search rule applied to that text, written once and used for both years. An identity step counts when identity verification, a photo identification or an identity check sits in the same sentence as the hiring process, a candidate, an interview or onboarding. The federal I-9 formula ("all persons hired will be required to verify identity and eligibility to work") does not count as an identity step. It falls under the E-Verify and I-9 line with other eligibility boilerplate. Background checks are counted apart from identity steps. Drug tests alone and work-authorization lines are not counted.

The rules were checked by reading postings. For each measure we read 20 randomly chosen matching postings. All 20 were correct for identity steps, interview requirements, fraud screening, scam warnings and eligibility lines, and 19 of 20 for background checks. The one error, a scam warning that listed background checks among fees, is excluded by the final rule. We also read 22 near misses for each measure below, postings that came close to matching but did not. For interview requirements, 1 of 22 should have counted: an in-person interview listed as a stage without requirement wording. Fraud screening missed 1 of 22. Identity steps, background checks and scam warnings missed none.

A posting cannot show the screening that actually happens, or anything after the posting: the interview itself, the check a vendor runs, or a warning sent by email. A posting that names no step may still run one. No causal claim follows from these rates. This read covers security job postings only, although the question applies to every job. A version across all jobs will follow once the collection covers every job description.

8 How this answer was stress-tested

Table 4: How this answer was stress-tested.

Test	Identity or interview step	Scam or impersonation warning	Background check
Headline, 2026 rate and change	2.5% (+0.8 to +4.8)	11.3% (+7.1 to +14.5)	6.2% (−1.4 to +4.7)
Two largest employers removed	1.2% (+0.5 to +2.1)	9.7% (+6.2 to +12.3)	4.9% (−2.1 to +2.7)
The same companies, 74 with postings in both years	6.3% (+0.0 to +15.9)	13.7% (+1.0 to +20.7)	3.9% (−5.9 to +4.9)
Staffing firms and government contractors removed	1.8% (+0.6 to +3.4)	11.6% (+7.2 to +14.9)	6.3% (−2.0 to +4.4)
Postings of 3,000 to 6,000 characters	0.9% (+0.1 to +2.0)	5.0% (+2.2 to +8.1)	4.9% (−5.1 to +2.7)
2024 postings applied through a company job board	2.5% (+0.8 to +4.8)	11.3% (+3.9 to +13.8)	6.2% (−6.3 to +4.5)
Each employer counted once	2.2% (+1.2 to +3.1)	9.7% (+6.8 to +11.0)	8.3% (+0.3 to +5.4)

Source: AKA Security analysis, likely ranges (95%) in percentage points, resampled by company. Each cell shows the 2026 rate in that check, then the change from 2024. In the identity column, the same-companies check shows no clear change, and 3 employers account for every match there. Fraud screening shows no clear change in postings of similar length (−0.4 to +1.5).

9 What would strengthen this answer

Table 5: What would strengthen this answer.

Test	What it would settle	Why it has not run
Full closing text from every board	Whether Lever employers carry warnings the data misses	Lever postings in this data hold almost no closing text.
A 2026 LinkedIn sample	Removes the difference in collection method	No public 2026 LinkedIn dataset exists.
More employers naming identity steps	Whether the rise is broad rather than carried by a few employers	18 employers name one today.
What happens after the posting	Whether a named step is carried out, and how often an unnamed one runs	Postings cannot show it. It needs employer or candidate reports.

Acknowledgements

Question asked by [Evan Wolff](#).

References

- [1] AKA Security Research Factory. *Security Hiring Research: What Job Postings Say About Security Work*. AKA Security, 2026. akasecurity.io/research/security-hiring-research
- [2] DataStax. *LinkedIn Job Postings* (datastax/linkedin_job_listings). Hugging Face dataset, 2024. huggingface.co/datasets/datastax/linkedin_job_listings

Cite as

```
@techreport{aka-rz-2026-10,  
  title      = {How Are Security Job Postings Screening and Authenticating Candidates? Scam Warnings Rose,  
and a Few Employers Now Name Identity Checks},  
  author      = {{AKA Security Research Factory}},  
  institution = {AKA Security},  
  type        = {Research report},  
  number      = {AKA-RZ:2610.10v1},  
  version     = {1.0.0},  
  year        = {2026},  
  month       = oct,  
  url         = {https://akasecurity.io/research/candidate-screening-and-authentication}  
}
```