

The LinkedIn Job Search Safety Pulse: 2026

May 2026



1: Why job search safety matters now: The scale of employment scams in 2026

For many people, encountering scams is now an everyday reality. Global Anti-Scam Alliance [research](#) shows that **70%** of adults worldwide encounter scams each year, with 13% exposed daily.

Employment scams are [escalating fastest](#). **Federal Trade Commission (FTC)**, data shows losses linked to job offers have surged, reaching hundreds of millions of dollars most years.

This report reflects how job seekers feel today, and the steps being taken to help them navigate their search with greater confidence and safety.

72%

of professionals surveyed say they stop to think about the legitimacy of a role at least sometimes before applying

2: How job-seekers experience job scams today

Spotting scams is now a routine part of the job search

New research from LinkedIn shows that questioning whether a job is “actually real” has become a routine part of the job search. Nearly three-quarters (**72%**) of professionals surveyed say they stop to think about the legitimacy of a role at least sometimes before applying, including 29% who say they always do.

That caution is growing, **57%** of professionals say they are more likely to question whether a job is a scam than they were a year ago, compared with just 11% who say they are less likely to do so. Recruiters are experiencing this caution too: **49%**¹ say job seekers have proactively reached out to check whether a role is genuine.

The trust signals job seekers rely on most

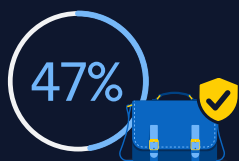
People are essentially looking for 'proof of life' before they apply. The biggest trust signal is the company's own reputation (**29%**), but the environment where they find the job is a close second (**28%**). They're looking for detail, clarity and signals tied to the person posting the job, such as whether the recruiter looks real or has a verified badge.



Job-seekers are most likely to check for these signals



search for the company or role online



check whether the job appears on the company's own careers site



review the company's LinkedIn Page



look for verification on the company, recruiter profile, or job posting itself

Which trust signals to job-seekers check?

70%

of recruiters say verification of the job, recruiter or Company Page is now a must-have

Recruiters are responding to this by helping to give job seekers more confidence: **68%** are actively taking steps to build trust with candidates, and **70%** say verification of the job, recruiter or Company Page is now a must-have.²

From first message to job offer: where job seekers feel most vulnerable

The hardest part of a job search isn't just the interview, it's the uncertainty before you even apply. For many, that 'vulnerability window' opens the second they start browsing. **22%** say they feel most worried about scams when browsing jobs, and another **21%** when they first receive outreach from a recruiter or company. This reinforces that trust isn't built during the job offer; it's won or lost in those very first seconds of contact.

90%

of reported scam messages involve moving to private messaging

A major red flag is being asked to leave LinkedIn for a personal chat app. LinkedIn data shows that **90%³** of reported scam messages involve moving to private messaging, where LinkedIn's safety tools can't protect you and accounts are far more difficult to verify. In fact, **over half** of all off-platform attempts happen in the very first message, before any meaningful context or trust has been established.

The clearest red flags that professionals surveyed are aware of are



How aware are job seekers of common red flags?

Gen Z are most exposed to job scams but least likely to see it coming

Younger professionals are encountering job scams more often than other generations, and are more likely to report falling for one, 32% of Gen Z say they've been a victim compared to 17% of Gen X. But the data points to a deeper vulnerability: not just a lack of caution, but a gap in knowledge of the specific tactics scammers use.

32%

of Gen Z admit to ignoring warning signs simply because they feel opportunities are so scarce

The real danger zone is caused by the combination of lack of awareness and pressure. While older generations are often better at spotting 'red flags,' Gen Z is facing a much harsher reality. In a crowded and competitive job market, many feel they can't afford to be skeptical. In fact, **nearly a third of Gen Z (32%) admits to ignoring warning signs** simply because they feel opportunities are so scarce. Compare that to just 21% of Gen X and only 8% of Baby Boomers, and you start to see the true cost of today's job hunt: for many young professionals, the need for a break is outweighing basic security checks.

Percentage of professionals who question common 'red flags'



	Gen Z (18-28)	Gen X (45-60)
Being asked for an upfront payment (e.g. to purchase a laptop)	40%	58%
Pressured to make a quick decision	34%	47%
Phone call without context	27%	37%
Asked for sensitive information, like bank details, early in the process	54%	59%

Generational differences between awareness of red flags

That gap between exposure and perceived risk, compared to knowledge of risky tactics leaves younger job seekers particularly vulnerable, especially during early-stage outreach when scams most often begin.

Time, money and trust: what job-seekers really lose to job scams

We often talk about the financial cost of scams, the sheer volume of them is what's truly disruptive. Most professionals (**62%**) report having seen a job they suspected was fraudulent. With **21%** already having been a victim and another **30%** reporting a close call.

Among those impacted, the most common consequences include



The most common consequences of job scams

These job scams are also impacting recruiters: **36%** of recruiters say they've been victims of impersonation, and **67%** say jobs scams are making it harder to build trust with candidates.⁴

3: How LinkedIn Protects Against Job Scams: Detection, verification and protection: LinkedIn's three-layer defense against job scams



1: Detection: Blocking Scams Before Members See Them

The most effective protection happens before a scam ever reaches job seekers. By layering automated defenses with human oversight, the vast majority of harmful content is intercepted at the gate. LinkedIn uses a combination of automated technology and human review to detect and remove scam activity at scale, stopping harmful content early and reducing risk during vulnerable moments.

- 98.7% of detected spam and scam content is removed by automated defenses before it's seen by members
- 99.5% of detected fake accounts are stopped proactively, before being reported⁵

LinkedIn's three-layer defense



2: Verification: Confirming Real Companies, Candidates and Recruiters

In a crowded market, knowing who is on the other side of a job post or application is half the battle. Verification tools, like those offered by LinkedIn, are designed to help remove the "guesswork" from professional outreach between candidates and recruiters:

- **Verification badges:** on recruiter profiles and Company Pages give job seekers access to trust signals about the jobs they may be interested in applying for.
- **Verification on Jobs:** helps signal that there is verified information about the company or job poster that's been confirmed by LinkedIn or one of our trusted third-party partners, reducing uncertainty before applying. Recruiters will also be required to verify anytime they edit or add a new experience related to hiring.
- **Verified Applicant Spotlight:** shows verification badges in LinkedIn hiring products, so recruiters can quickly discover and spotlight applicants with verified identities.
- **On platform security:** Applying and communicating on LinkedIn for applications and messaging helps job seekers stay within built-in security protections.
- **Community watch:** Direct reporting tools allow job seekers to flag suspicious activity, creating a safer community for everyone.



3: Protection: Strengthening the Job Search Experience

Safety is a moving target, which is why the defense layers LinkedIn has added have become more sophisticated and less intrusive.

- **Guardrails requiring verification** for high-risk job posters.
- **Reduced visibility** of posts and comments that may be more likely to be scams, for example containing suspicious links.
- **Smart spam filtering** with suspected scam messages sent to junk folders so you can focus your inbox on real opportunities.
- **Frictionless security** with expanded two-factor authentication and behind the scenes detection, increasing account protection that works in the background to maintain safety in the job search.

LinkedIn's three-layer defense

Beyond scams: reducing uncertainty in the job search

Security is one side of the coin, the other is clarity and transparency. Today's job search shouldn't feel like a black box. By providing more context about roles, companies and fit, you can make more confident decisions.

- **LinkedIn Hirer insights:** [A tool](#) which provides signals that help job seekers understand what's happening with a role — reducing guesswork and uncertainty.
- **LinkedIn Job Match:** [A tool](#) which highlights exactly how a candidate's experience and skills align with a job role, helping them focus on high probability, legitimate opportunities.
- **LinkedIn Job Tracker:** [A tool](#) which provides a single, organized view into where you stand across applications. By mapping out progress and next steps in one place it removes "where do I stand?" anxiety that often follows applying.
- **Human centered accountability:** People-led hiring signals in jobs tracker bring a face to the process. Showing a real recruiter, hiring manager, or shared connection attached to a role, including in saved jobs within Job Tracker, adds accountability, context, and trust.



4: How to Stay Safe During Your Job Search: A Practical Checklist for Job Seekers

As job scams become more sophisticated, staying safe means knowing when to slow down and what signals to look for, especially in the earliest stages of contact.

- ✓ **Stay on-platform for early-stage conversations:** Scammers often try to move conversations off LinkedIn quickly. By staying on-platform for those first few chats, you're backed by built-in protections, reporting tools, and trust signals, making it easier to assess whether a role or recruiter is legitimate before engaging further.
- ✓ **Do a quick identify check to verify who you're dealing with:** Before applying or responding to outreach, take a moment to feel more confident about who you're interacting with by checking:
 - The company's LinkedIn Page
 - The recruiter or poster's profile
 - Whether the role appears on the company's own careers site
 - Any available verification badges on the company, job or recruiter
- ✓ **Trust your gut at the "vulnerability moment":** The earliest moments of contact are when people feel most at risk. Pressure to act quickly, vague job details, or unexpected outreach can all be signs to pause. Real opportunities don't disappear because you took a beat to think.
- ✓ **Keep your sensitive info private:** A legitimate employer won't ask for sensitive personal information, identity documents, or upfront payments at the start of a hiring process.

See something. Say something. If something doesn't feel right, or a message feels off, report it directly. It only takes a few seconds. On LinkedIn you can do this via the 3 dots above a job posting.

Key Takeaways: What Job Seekers and Recruiters Should Know

- Employment scams are most likely to occur during first contact
- Gen Z faces the highest exposure but lowest perceived risk
- Off-platform redirection is a primary scam tactic
- Verification and on-platform engagement meaningfully reduce risk

Key takeaways for job seekers and recruiters

Methodology

The research was conducted by Censuswide, among a sample of 8512 Professionals (working full or part time) (Aged 18+) across the UK, USA, India, Germany, and Brazil. The data was collected between 16.03.2026 - 30.03.2026. Censuswide is a member of the Market Research Society (MRS) and the British Polling Council (BPC), and a signatory of the Global Data Quality Pledge. We adhere to the MRS Code of Conduct and ESOMAR principles.

¹ Those who are involved in the recruiting process

² Combines 'Strongly agree' and 'Somewhat agree'

³ Source: LinkedIn Platform data, January 2026

⁴ Combines 'Strongly agree' and 'Somewhat agree'

⁵ Source: LinkedIn Transparency Report, January-June 2025