

Hey! What's New? 2025-69

Recruitment fraud: What You Need to Know

Rhymer Rigby writes, in the latest issue of the *Journal of Accountancy*, that “recruitment fraud has become a real problem across many industries, including the finance sector. Also known as a job scam, recruitment fraud involves criminals posing as legitimate employers, recruitment consultants, and so on. It’s not a new problem, but a growing one, and it goes hand in hand with technological advances ranging from smartphones to AI. So, what do you need to watch out for and how do you protect yourself — and what should employers know?”

What are the scammers after? Usually, says Rigby, it’s one of two things. “The first is money, and the second is personal information. The motivation for money is obvious. Information is slightly more complex. This is often used for identity theft. People who steal your identity can use it to apply for bank accounts and credit cards, attempt to take over your existing accounts, sell your information on the dark web or blackmail you.”

Recruitment scams vary widely. Rigby says they can range from fake job listings to SMS texts to people (and even AI deepfakes) posing as executive recruiters calling individuals and claiming to work for legitimate companies. “Some are relatively easy to spot, but others, such as fake recruiters, premium phone line scams (where you are asked to call a number that incurs very high charges) and fake job-site listings, may be very difficult to spot.”

Some scams are pretty basic. “There might be poor spelling or grammar in the communications. You may be asked to click on a dubious-looking link. And the scammer might only be willing to give out a mobile number or a personal email address.” But anything that seems too good to be true should also be suspect, Rigby warns “but, increasingly, job scams can feel very convincing — it is surprisingly easy to put together a very professional-looking approach, which then takes real effort to spot, and technology has made targeting and customization much easier.”

The most obvious scam is asking for money upfront. Rigby notes that you will usually be given a reason, for example, to pay for a background check or as an “admin fee.” “Legitimate recruiters do not ask for money in this way. You might also be asked for a scan of your passport or driver’s license “for security.”

Some scammers play a much longer game, though, he says. “They may string you along through a series of emails and even fake interviews and, once they’ve gained your trust, they then tell you they need your bank details to set up salary arrangements. Conversely, they may simply harvest a lot of information about you — and that’s the last you’ll hear from them until a debt collector starts chasing you for the bills the scammers have run up on the credit cards they took out in your name.”

Rigby suggests that “common sense is your best first line of defense. If someone calls you out of the blue and asks you to make a snap decision or starts asking for details, get their name and tell them you’ll call them back. If they refuse or start pressuring you, they’re likely a scammer.”

Research the people who contact you, Rigby advises. “Can you find them on LinkedIn or, better still, a company website? If it’s a recruiter you haven’t heard of, do they have a physical address and a landline phone number? Finally, trust your gut. If something feels off, there’s a good chance it is.”

LinkedIn is, however, “fertile ground for recruitment scammers. In the first half of 2024, LinkedIn removed more than 86.5 million fake accounts and over 142 million scams and spam content. It’s very easy to pose as a legitimate recruiter, and platforms like LinkedIn add a layer of credibility.”

While employees should be alert to the problem, so should employers, Rigby suggests. “They should implement robust protocols, raise awareness, and take precautions. Organizations need to make it very clear within their industry what candidates should expect in terms of approach, job advertising, and process. Organizations should educate their own HR departments, use appropriate technologies to secure their processes and combat fraud, and be responsive to anyone who has questions. They should also work with governments, law enforcement and recruiters.”

What does the future hold? Potentially, far worse, says Rigby. “AI can already fake people’s voices and faces, write fake job ads at scale, create bogus photos, and even conduct some virtual interviews. We may soon face a future where the only way to be certain that the person you’re speaking to is real is to meet them in the flesh.”

For considerably more, check out [Recruitment fraud: What you need to know](#).