Hey! What's New? 2025-12

Recruitment Fraud: What You Need to Know

Rhymer Rigby writes in a current issue of *FM Financial Management* that recruitment fraud (or job scams) has become a real problem across many industries, including the finance sector. "Quite simply, it is where fraudsters pose as legitimate employers, recruitment consultants and so on. It's not a new problem but a growing one and 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, Rigby asks. "Usually, 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 fraud (using CVs, employment records, and so on) can be a particularly rich source of information and allow for very convincing impersonations."

Recruitment scams vary widely, Rigby explains. "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 clues 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. Anything that's too good to be true should also be suspect."

Rigby also describes some of the scammers' favourite methods? "The most obvious one is asking for money upfront. 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.'"

But, Rigby adds, "some scammers play a much longer game. 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 in order 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 they've run up on the credit cards they took out in your name."

He advises that common sense is the 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. With emails, check the sender's address and whether the messages look and feel legitimate. Don't click on links if you have any questions about them. Research the people who contact you. 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 landline phone number? And, also, trust your gut. If something feels off, there's a good chance it is."

Scammers have a toolbox of mind tricks designed to make you do what they want — whether it's divulging passwords, sending money or scanning a passport. According to Rigby, a classic one is giving you a time limit. The scammer might say, "Applications for this vacancy close today — you need to pay me $50 now so I can do the background checks." This puts pressure on you to make an immediate decision and also plays to the loss-aversion bias (where avoiding a loss is prioritized over an equivalent gain)."

While employees should be alert to the problem, so should employers, Rigby advises. "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? Rigby warns that it could, potentially, become far worse. "AI can already fake people's voices, 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 more, see Recruitment fraud: What you need to know.