FMBusinessDaily

Struggling Young Jobseekers Warned as Fake AI Job Adverts Surge – Expert Reveals Warning Signs

3 hours ago

Following reports of AI-generated fake job adverts impersonating major brands like Spotify and Meta, CV-Library, the UK's largest independent job board, is warning jobseekers to stay vigilant as scams grow increasingly sophisticated.

Designed to look like real hiring processes, scam adverts direct applicants to fake websites that prompt users to log in with their social media or email accounts, allowing fraudsters to steal their details. Once hacked, there's a risk of exploitation, targeting friends and family, and even requesting money. Interest in the issue is also rising, with UK Google searches for "job scam" reaching its highest point in the past month, according to Google Trends data.

These scams target some of the UK's most vulnerable jobseekers – young people struggling to enter the workforce. Youth unemployment has risen to 15.8%, up from 14.6% a year earlier, with 713,000 people aged 16-24 unemployed, making awareness of job scams more important than ever.

Katie Emerton, Recruitment Expert at CV-Library said: "Younger jobseekers are particularly exposed to these scams, often applying to dozens of roles at once. With AI making fake job adverts increasingly difficult to distinguish from genuine listings, knowing how to verify both the role and where you're applying is vital.

"Applying through official channels should be the first step. At CV-Library, we run multiple verification checks before a role is published, including confirming the business is legitimate, UK-based and properly

registered. We also speak directly to employers, giving candidates confidence that the role, and the company is genuine.

“Importantly, all job postings on our site are paid for, which helps significantly reduce the risk of fraudulent listings appearing in the first place.”

6 ways to verify if a job is real

1. Apply via official websites or trusted job boards only – scammers often copy real listings but redirect applicants to fake websites designed to steal data or money. If you’re sent to an unfamiliar link or external form, apply directly via the company’s website or a trusted job board where roles are verified.
2. Never share personal or login details early in the process – legitimate employers won’t ask for sensitive information such as passport number, bank details, National Insurance number or social media credentials. Requests like these are major red flags and could indicate identify theft.
3. Don’t rely on social media job ads – social media might be used to promote roles, but they shouldn’t be your only source. Always cross-check the job on the company’s official careers page or a reputable job board before applying.
4. Be cautious of fast-track hiring – job offers with little or no interview process should raise alarm bells. Genuine roles will involve multiple stages, while scammers use urgency to stop candidates from properly vetting the opportunity.
5. Check domains carefully – look closely at website URLs and email addresses. Small changes, such as extra letters, hyphens, or unusual endings, can signal it’s fake, even if the website looks professional.
6. Be wary of WhatsApp messages by recruiters – while some recruiters may use messaging apps, unsolicited job offers or requests for personal information should be treated with caution. Always verify the recruiter and company before engaging.