# Rise in sophisticated online scams prompts urgent public awareness campaigns



In an era where digital communication is integral to daily life, scams across platforms like WhatsApp, LinkedIn, and Gmail have become increasingly sophisticated and prevalent, targeting vulnerable individuals with alarming persistence. Recent warnings from various authorities and consumer protection groups reveal a growing spectrum of fraudulent schemes exploiting everything from job searches to government benefit claims, alongside scams impersonating regulatory bodies.

One prominent example involves fraudsters masquerading as the Financial Conduct Authority (FCA), the UK's financial regulatory body. The FCA has reported thousands of impersonation attempts this year alone, with nearly 4,500 scam reports in the first half and approximately 480 individuals falling victim by sending money or sensitive financial details to these criminals. Notably, over 60% of these cases involved victims aged 56 or older. Common tactics include false claims of recovered funds from illicit crypto wallets opened in the victim's name or promises to help recover losses from loan scams—methods designed to instil trust and prompt additional payments. The FCA emphasizes it will never request funds or sensitive banking information and urges vigilance.

LinkedIn, a key platform for professional networking and job hunting, faces a surge in scams targeting job seekers. Fraudulent CV-writing services have emerged as the largest threat on the platform, constituting over a third of job-related scams globally. These services often deliver substandard or AI-generated CVs for a fee while putting users' personal data at risk, especially as scammers encourage conversations off-platform where LinkedIn's oversight is reduced. This spike coincides with the recruitment surge typical of September when new graduates and returning workers increase hiring activity. LinkedIn has responded by introducing a verification system for recruiters that displays a checkmark to confirm authenticity; however, the effectiveness of this measure has been questioned, with reports of fake job ads and scams persisting despite these tools. Job hunters are advised to watch for red flags such as fake profiles, vague job descriptions, unsolicited offers with too-good-to-be-true promises, requests for sensitive information early in the process, and the use of personal rather than corporate email addresses.

Beyond job scams, Gmail users have been warned about a new phishing plot involving fraudulent messages and calls pretending to be from Google Support. The attackers attempt to capture security codes sent during password reset processes, enabling immediate access to victims' accounts.

WhatsApp has also been exploited for job scams, with messages promising high daily earnings for remote roles at companies like TikTok. These scams lure victims into initial “easy” tasks such as completing surveys, followed by requests for investment money that cannot be recovered.

Online retailer Temu has been impersonated in scams involving emails that offer e-bikes in exchange for completing surveys about shopping experiences. These emails, containing malicious links, are designed to harvest personal and financial information.

Winter Fuel Payment scams have taken advantage of the government’s support programs for vulnerable populations, with fraudsters posing as officials or energy providers to extract personal or bank details under the guise of processing payments. Official communications never request passwords, PINs, or bank card numbers via unsolicited contact.

Mobile network customers, particularly EE users, have been targeted with phishing texts claiming failed direct debits. These messages include links to counterfeit sites aimed at stealing personal and payment details.

The increasing sophistication and volume of such scams highlight a pressing need for public awareness and caution. Regulatory bodies like the FCA are stepping up efforts to crack down on deceptive financial promotions, including those by social media influencers, who often lure younger audiences into risky investments under false pretences. Barclays has reported a 30% rise in investment scams, with victims suffering significant losses. Consumer advice consistently stresses skepticism towards unsolicited offers, thorough verification of sources, and reliance on professional financial counsel.

For job seekers, especially on platforms like LinkedIn, vigilance remains vital. In addition to LinkedIn’s verification measures, recognising typical scam behaviours—such as pressure tactics, poor communication quality, and requests for upfront payments—can safeguard candidates against fraudulent schemes. Experts also advise conducting independent research and consulting trusted sources before engaging with unfamiliar recruiters or offers.

As scams evolve alongside digital tools, consumers must stay informed and cautious. Awareness of common tactics and verification of identities can reduce the risk of falling prey to these increasingly complex frauds.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651), [[4]](https://www.businessinsider.com/fake-check-job-scam-linkedin-recruiter-verification-tools-2024-5)
* Paragraph 2 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651), [[2]](https://www.ft.com/content/6f5055fc-08f6-4d83-9b66-414f7f09971e)
* Paragraph 3 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651), [[3]](https://www.axios.com/2024/04/09/linkedin-recruiters-job-scams), [[4]](https://www.businessinsider.com/fake-check-job-scam-linkedin-recruiter-verification-tools-2024-5), [[5]](https://www.safetydetectives.com/blog/linkedin-job-scams-protect-yourself/)
* Paragraph 4 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651)
* Paragraph 5 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651)
* Paragraph 6 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651)
* Paragraph 7 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651)
* Paragraph 8 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651), [[2]](https://www.ft.com/content/6f5055fc-08f6-4d83-9b66-414f7f09971e)
* Paragraph 9 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651), [[3]](https://www.axios.com/2024/04/09/linkedin-recruiters-job-scams), [[4]](https://www.businessinsider.com/fake-check-job-scam-linkedin-recruiter-verification-tools-2024-5), [[5]](https://www.safetydetectives.com/blog/linkedin-job-scams-protect-yourself/), [[6]](https://www.maketecheasier.com/common-linkedin-scams/)
* Paragraph 10 – [[1]](https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651), [[2]](https://www.ft.com/content/6f5055fc-08f6-4d83-9b66-414f7f09971e), [[5]](https://www.safetydetectives.com/blog/linkedin-job-scams-protect-yourself/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.liverpoolecho.co.uk/news/uk-world-news/whatsapp-linkedin-gmail-scams-you-32359651> - Please view link - unable to able to access data
2. <https://www.ft.com/content/6f5055fc-08f6-4d83-9b66-414f7f09971e> - UK regulators, led by the Financial Conduct Authority (FCA), are intensifying efforts to curb financial promotions by influencers amid rising fraudulent social media investment schemes. Recent charges against former reality TV stars for unauthorized promotion of high-risk foreign exchange schemes via Instagram exemplify this crackdown. In 2023, the FCA removed 10,000 deceptive financial promotion ads, up from 8,500 the previous year. Investment scams, heavily promoted on social media, have surged, with Barclays reporting a 30% increase and significant average losses. Influencers' promotion often misleads younger investors, overshadowing professional financial advice. Regulatory and consumer advocacy groups recommend skepticism and reliance on trusted financial advice sources.
3. <https://www.axios.com/2024/04/09/linkedin-recruiters-job-scams> - LinkedIn has introduced a new verification process to combat recruiter scams, as generative AI tools have made it easier for scammers to deceive users with fake job offers and collect sensitive financial information. Verified recruiters will now display a checkmark badge confirming their authenticity. LinkedIn claims it already intercepts most fake accounts before they are reported, and the verification aims to provide users with greater transparency and control for making informed decisions. Currently, LinkedIn verification is not available in all markets, but the rollout of the feature will begin this week with plans to expand globally.
4. <https://www.businessinsider.com/fake-check-job-scam-linkedin-recruiter-verification-tools-2024-5> - LinkedIn rolled out verification tools last year to curb spam and fake job ads on the platform. So far, it doesn't appear to have worked. Job hunters say fake ads from scammers are still rampant on the site. The scams often target recent graduates and young professionals, per the Federal Trade Commission. Despite the new process, it doesn't appear to have worked. The scams often target recent graduates and young professionals, per the Federal Trade Commission.
5. <https://www.safetydetectives.com/blog/linkedin-job-scams-protect-yourself/> - To protect yourself from LinkedIn job scams, it’s important to know the red flags. Here are the most common signs that a job offer or recruiter on LinkedIn might be fake: Suspicious profiles. Scammers often create fake LinkedIn profiles that lack essential details. Watch out for incomplete work histories, low connection counts, and stock images or missing profile pictures. Another telltale sign is an unusually high number of endorsements that don’t match the person’s work experience. Too-good-to-be-true job offers. Be wary of unsolicited job offers that promise extremely high salaries for minimal work or provide unrealistic perks. Legitimate companies rarely offer senior-level compensation for entry-level positions. Trust your gut — if it seems too good to be true, it probably is. Vague job descriptions. Scammers often use generic language to cast a wide net. If you can’t pinpoint what the job actually entails or the message sounds like it wasn’t written specifically for you, it’s likely a mass-sent scam. Requests for upfront payments. No legitimate company will ask you to pay fees to apply or get hired. If you’re asked to purchase equipment or software before starting a job, with promises of reimbursement later, it’s most likely a scam. Pressure tactics and urgency. Scammers often create a sense of urgency to get you to act without thinking — be cautious of messages that push you to make quick decisions. Poor grammar and spelling. While everyone makes mistakes, frequent grammatical errors and typos in job postings or recruiter messages are red flags. Legitimate companies typically maintain high standards in their communications. Requests for sensitive information. Be extremely cautious if asked for personal data like your Social Security number or copies of government-issued IDs early in the application process. Legitimate employers only request this information after you’ve accepted a job offer. Use of personal email accounts. Real recruiters and hiring managers will contact you via official company email addresses. Messages from Gmail, Outlook, or other personal accounts should be treated with suspicion. Interviews over messaging apps. If a recruiter insists on conducting interviews via WhatsApp, Telegram, or other messaging platforms instead of in-person or through video conferencing, it’s likely a scam. No company LinkedIn page. While not definitive proof, the absence of a LinkedIn page for the company a recruiter claims to represent is cause for concern. Legitimate businesses typically maintain a presence on the platform. Remember, staying vigilant and recognizing these red flags can help you avoid falling prey to LinkedIn job scams. If something feels off, take a step back and thoroughly research the company and position before proceeding. Being cautious could save you from potential financial loss and identity theft.
6. <https://www.maketecheasier.com/common-linkedin-scams/> - Cryptocurrency is the digital gold rush of our time, offering promises of quick riches and financial freedom. The sector has attracted an alarming number of fraudsters. Nowadays, cryptocurrency investment scams on LinkedIn represent a significant threat to user safety. Typically, a so-called “crypto expert” connects with a LinkedIn user and starts engaging in small talk. Gradually, the conversation shifts to investment opportunities in the crypto space. Those who entrust their investments to these fraudsters always see their money vanish into thin air. Common Warning Signs: Amazing cryptocurrency investment opportunities never come knocking on your door, so be wary of anyone who reaches out unsolicited. Over-the-top promises of high returns on investment in a short period. Urgency in their messages, pressuring you to invest as soon as possible. Defensive Measures: Never invest in a scheme solely based on someone’s recommendation on LinkedIn. If the offer seems too good to be true, that’s usually a sign to stay away. Always perform your own research and consult with authorized financial experts.
7. <https://www.latimes.com/business/story/2023-01-12/job-scams-skyrocket-linkedin-indeed-pandemic> - Others have also reported encountering fake recruiter profiles for legitimate companies on LinkedIn and other job search sites such as Indeed. Heather Lagaso, 42, has been on the hunt for a remote job since her role in compliance and records management at the Oregon Occupational Safety and Health division was cut in November 2021. In 2022, she encountered 67 fraudulent job postings, almost all on LinkedIn or Indeed, she said. She’s been keeping track of the listings in a document she shared with The Times. “I was honestly looking for anything that offered ... a home schedule or some sort of flexibility with it,” due to her son’s medical needs, said Lagaso, who lives in Gervais, Ore. She noticed many of the jobs were in customer service, personal assistance or things involving logistics or dispatch. Some scams were obvious, but others were tougher to spot — including one that involved a web address similar to the real company’s domain name, she said. In that case, she applied through LinkedIn and was asked to download an app called Wire for further communication.