People Are Being Bombarded With Strange Job Offer Scams – Here's What A Cybersecurity Expert Wants You To Know

buzzfeed.com/beccamonaghan/scam-calls-whatsapp-job-offers-explained

Becca Monaghan September 24, 2026

"The scammer wants somebody to answer, show an interest, and then move the conversation somewhere they can keep it going."

Remember when scam calls were "Congratulations, you've won £10,000"? Well now, they've had a rebrand. The latest pitch is seemingly "We have a job for you", which feels considerably more believable – and somehow a more depressing sign of the times.

0:00

It's not just one dodgy number doing the rounds. People say they're now getting several a day from different mobile numbers. Of course, we all want to know: where the hell are they getting our details from?

> you know the state of the uk is bad when scam calls aren't even like "hey you've won the lottery" or "hey this is the government you need to pay a fine" but are "hey, we have a part time job opportunity"
>
> — franzi ₊˚⊹ 🎀 (@Killdeerrr) September 17, 2026

franzi ₊˚⊹ 🎀 / Via x.com

> THESE UK SPAM CALLERS LITERALLY START THE CALL BY SAYING "we have a job for you" OH THEY KNOW HOW DESPERATE PPL ARE 😭😭😭😭😭😭
>
> — seraphine ★🍉 (@yrinsanelove) September 20, 2026

seraphine ★🍉 / Via x.com

> Job market is so cooked that the most common scam call I receive these days are automated voice recordings offering up part time work
>
> — Calum (@reds_cp) September 21, 2026

Calum / Via x.com

So, what's actually going on? We spoke to a cybersecurity expert to find out where these calls and messages could be coming from and what you should do if you get one.

Bringing it back to basics, Kevin Walker, founder and senior security consultant at Black Swan Cyber Security Solutions, explains that just because a call appears to be coming from a normal UK mobile number, that doesn't necessarily mean it actually is.

"Caller ID can be spoofed. In fact, Ofcom has specifically been tightening the rules around overseas calls being made to look as though they are coming from UK mobile numbers," he tells *BuzzFeed*.

And while answering the call isn’t necessarily an instant threat, Kevin likens it to a "knock on the door".

"The scammer wants somebody to answer, show an interest, and then move the conversation somewhere they can keep it going," he explains.

WhatsApp can then make that particularly easy, he adds: "They can message repeatedly, send links, introduce supposed recruiters or managers, and gradually make the conversation look more convincing."

0:00

And the whole "we have a job for you" angle feels particularly pointed right now. The UK job market has become increasingly difficult, with the number of available jobs now at its lowest level in more than five years, according to the Office for National Statistics (ONS). The ONS also found that some smaller businesses are being affected by rising labour and operating costs.

According to Kevin, that's exactly what can make a job offer an effective hook.

"We've seen recruitment scams where what starts as apparently easy, flexible work eventually turns into requests for money, purchases, deposits, or personal information," he explains.

And scammers don't need everyone they contact to fall for it. Kevin describes the approach as a "numbers game": "They only need a small percentage of people to think, 'I was looking for work recently, maybe this is genuine.'"

0:00

Naturally, some people have wondered whether a data breach could be behind the sudden influx. Kevin says it's "certainly one possibility", but he "wouldn't jump straight to that conclusion".

"Phone numbers can come from all sorts of places," he shares. "Previous data breaches, old marketing lists, scraped social media profiles, CVs and recruitment sites, compromised accounts, data that has been bought and resold, or simply automated attempts against large ranges of mobile numbers."

And the data doesn’t necessarily have to be recent: "A scam campaign starting this week could be using information that was leaked months or even years ago. Criminals collect data from different sources, combine it, and reuse it."

If a scammer appears to know specific information about you – such as where you work or that you’re actively looking for a job – Kevin says that "becomes more interesting and might suggest a more targeted data source."

But a vague WhatsApp message or a sudden increase in scam calls isn’t enough on its own to prove there’s been a data breach.

0:00

So, what do you do if you’ve already answered one of these calls?

First of all, don’t panic.

If you haven’t clicked anything, downloaded anything, shared passwords or verification codes, handed over personal or financial information, or sent money, Kevin says you’re unlikely to have put yourself in immediate danger.

"Simply answering a call doesn't mean your phone has suddenly been hacked," he states. "What you may have done is confirm that your number is active and that somebody responds to it, so I’d expect the possibility of more attempts."

The safest option is to end the conversation

"Block and report the WhatsApp account, and don’t click on any links they subsequently send you."

Ofcom also recommends using WhatsApp’s own reporting tools for suspicious messages, while suspicious SMS messages can be forwarded to 7726.

Check your WhatsApp privacy settings

"Limit who can see things such as your profile photo, status and other personal information."

0:00

"If you *have* clicked a link, downloaded an app, shared a password, given someone an authentication code, or sent money, that's a different situation, and you should act quickly. One of the phrases I use when talking about scams is: 'before you act, slow down. If you've already acted, move quickly.' But if you've simply answered "hello" or replied to a message before realising something wasn't right, there's normally no reason to assume the worst. Block it, report it and move on."

Additional thumbnail photo credits: Milan_Jovic/ArtMarie (iStock)