



Fraud warning: rise in fraudulent LinkedIn profiles

We are warning members of the public of an increase in fraudulent LinkedIn profiles impersonating Jersey Financial Services Commission (**JFSC**) employees and sending unsolicited connection requests.

These profiles may attempt to build trust before requesting sensitive information, promoting fraudulent investment opportunities, or directing individuals to fake websites.

JFSC employees do not use LinkedIn or any other social media platforms to conduct official business or communicate with regulated entities. Any such contact should be treated with caution. Individuals contacted via social media claiming to represent the JFSC should verify the contact independently before taking any action.

How to verify genuine contact from the JFSC

If you are contacted by someone claiming to represent the JFSC, including via social media, and have any doubt about their identity, do not share personal, financial, or sensitive information and do not act on unsolicited requests.

To verify that you are dealing with the genuine JFSC or its employees:

- only use the official website: www.jerseyfsc.org
- ensure emails are sent from the official domain: @jerseyfsc.org
- call the JFSC on [+44 \(0\)1534 822000](tel:+441534822000) and ask to speak directly to the individual who contacted you to confirm the communication is legitimate

Rise in impersonation scams

We continue to see an increase in impersonation scams. Criminals are becoming more sophisticated and often pretend to be:

- local professionals
- government authorities
- financial regulators
- well known organisations
- friends or family members

They may use real names, cloned websites, copied branding, and artificial intelligence generated images or voices. Their aim is to convince you they are genuine and pressure you into transferring money or sharing personal information.

How to spot a scam

If you receive an unexpected message, connection request, email, text, call or letter, look for signs that it may be a scam. These can include but are not limited to:

- spelling mistakes and poor grammar

- pressure and urgency for you to do something
- asking or telling you to click on a link
- unusual payment methods
- unusual communication methods
- promises or offers that seem too good to be true
- requests for sensitive and/or personal information
- website addresses and social media accounts that contain small changes from genuine sites

Fraud prevention resources

For further advice on avoiding scams and guidance on what to do if you think you may have been targeted, follow the Jersey Fraud Prevention Forum:

- Facebook: <https://www.facebook.com/jsyfraudforum>
- LinkedIn: <https://www.linkedin.com/company/jersey-fraud-prevention-forum/>

For further enquiries, please [contact the JFSC's Enforcement team](#).

You can also contact the JFSC's confidential whistleblowing line on [+44 \(0\)1534 887557](tel:+4401534887557).