

# New app to counter malicious approaches online

An innovative app, allowing users of social media and professional networking sites, to better identify the hallmarks of fake profiles used by foreign spies and other malicious actors, and take steps to report and remove them, has been launched today.

In the last year, over 10,000 UK nationals from across society have been targeted on sites such as LinkedIn and Facebook. The use of fake profiles on social media and professional networking sites is occurring at scale. In the first half of last year alone, LinkedIn stopped 11.6m fake accounts at registration.

The new app is part of the Centre for the Protection of National Infrastructure's (CPNI) 'Think Before You Link' campaign. It has been developed with behavioural scientists to include features such as a profile reviewer, which will help individuals identify potentially fake profiles and report anything they deem suspicious.

The launch of the app comes as increased espionage by state actors persistently threatens the UK, and is increasingly conducted online.

Chancellor of the Duchy of Lancaster Steve Barclay, Lead Minister for Cyber Security said:

The online threat via social media is increasing, with fake profiles on sites such as LinkedIn and Facebook being created on an industrial scale.

Many of these profiles are established as an elaborate ruse for eliciting details from either officials or members of the public who may have access to information relating to our national security.

It is therefore crucial that we do all we can to protect ourselves and our information, ensuring those who we connect with online are who they say they are. This new app will be an important tool in that endeavour.

Current and former civil servants can also be attractive targets because of their experience and if their positions are listed on sites such as LinkedIn, with this carrying the risk of fake offers of lucrative consultancy work if they connect with unknown users. This app will therefore boost the support and advice which government staff and particularly those working on sensitive policy, already receive.

New tools, such as the 'Think Before You Link' app, will enable users to

conduct their own digital due diligence and aims to increase awareness of the growing threat from digital espionage to UK citizens.

Director General of MI5 Ken McCallum said:

MI5 has seen over 10,000 disguised approaches on professional networking sites from foreign spies to people up and down the UK. Foreign spies are actively working to build relationships with those working in government, in high-tech business and in academia.

The Think Before You Link app helps those who may be receiving disguised approaches, helping them to conduct their own digital due diligence before accepting unknown contacts online.

Vincent Devine, the Government Chief Security Officer said:

Hostile actors can easily use social media to conduct online research into an individual's interests, activities and personal and professional connections. They can then use that information to target the individual online.

The Think Before You Link app is an effective way for government staff and the public to protect themselves against those threats.

### **Notes to editors:**

- The app is freely available to download on the Google Play or Apple store from today.
- New research released today by the University of Portsmouth suggests that around 16.8m LinkedIn users in the UK may have accepted unknown contacts and that awareness of the potential threat from state actors using fake profiles is lower than other potential online threats. When asked specifically about fake profiles and the motives of perpetrators more generally, users of LinkedIn and Facebook were most likely to think of trolling (80%), fraud (80%) and fake news (79%), rather than economic espionage (64%). Over half of users (53%) could not name a state that posts fake profiles. And yet, three quarters say they have knowingly received link requests from suspicious profiles.
- The University of Portsmouth's research was carried out by Professor Mark Button and Dr David Shepherd of the School of Criminology and Criminal Justice at the University of Portsmouth. It involved a survey of 1,000 UK professionals who use either LinkedIn or Facebook for professional networking. The survey data was collected in April 2022. For a copy of the report contact the University of Portsmouth press office: glenn.harris@port.ac.uk; for an interview with Professor Mark Button contact mark.button@port.ac.uk mobile: 07968 911405; work: 023 9284 3923.
- Click [here](#) for further information on the LinkedIn report.