Remember the four Rs to protect yourself against malicious profiles:

Recognise
a suspicious profile

Realise
the potential threat

Report
your concerns

Remove
them from your network

Know the signs

Too good to be true
You could be offered extremely flexible working arrangements or an eye-watering salary given the role advertised.

Lack of depth/detail
Google searches return a small online footprint and the role may reveal lack of tangible details.

Flattery
Overly focusing on your skills and experience along with a reference to government or 'high end' candidates.

Urgency
Overly responsive to messages, and attempts to rush you off the platform onto another communication method.

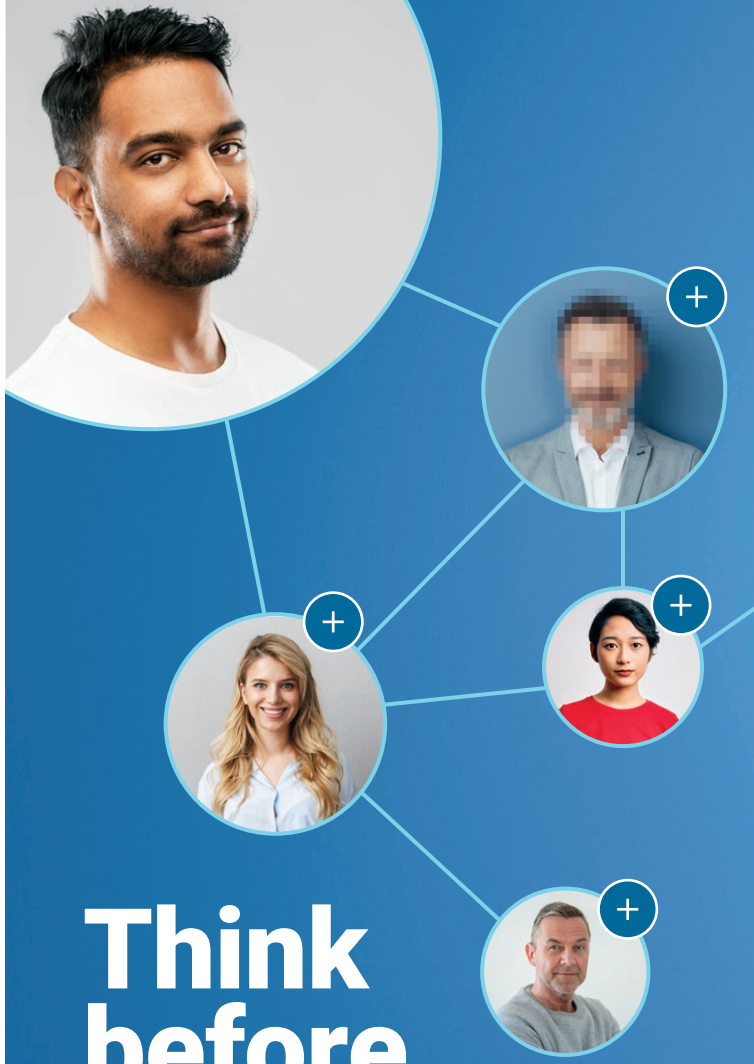
Exclusivity
Often you'll be tempted with a limited or one-off opportunity.

Imbalance
They do very little to validate your experience as a potential candidate.

What should you do?

- Review your account settings on social and professional networks so you can control the information that is available publicly – especially when it relates to security clearances
- Only form contacts online with people you know, or only after you have verified their identity is legitimate
- Report any contact from online profiles you suspect are malicious to your security team or person responsible for security in your organisation.

The information in this booklet is based on research carried out by the Centre for Protection of National Infrastructure (CPNI). CPNI is the government authority for protective security advice to the UK national infrastructure. www.cpni.gov.uk



Think before you link

Online networking – a guide to recognising when an online profile is malicious

PSR | Protective Security Requirements

Have you ever been contacted online by someone you don't know?

Professional and social networking sites are useful tools for promoting yourself, but can also expose you to unforeseen risks.

> *This guide will help you to recognise when an online profile and approach is fake and malicious, so you can protect yourself and your organisation from the harmful impacts of online exploitation.*

What is the threat?

Malicious individuals, criminals, and groups such as foreign state actors use social and professional networking sites to target and exploit people who may have access to sensitive or valuable information and resources.

Why are they doing this?

It's easier to disguise your true identity and intentions online. People with malicious intentions may use this approach to try to recruit you. They'll aim to get you to disclose sensitive or valuable information, so they can exploit it for criminal, social, economic, or political gain.

If you provide information, you could harm yourself and your organisation, or pose a risk to national security.

- The way you present yourself on social media could make you a target.
- Criminals are looking to exploit people who they identify as having high status positions with access to resources.

Who are they targeting?

You are at greater risk of being targeted if you:

- Disclose that you have access to classified or commercially-sensitive information, technology, or research
- Publicly disclose that you have a national security clearance.

How do they trick you?

Watch out for malicious actors:

- appealing to you through flattery
- offering you something you would find valuable
- trying to build rapport and develop a relationship with you.

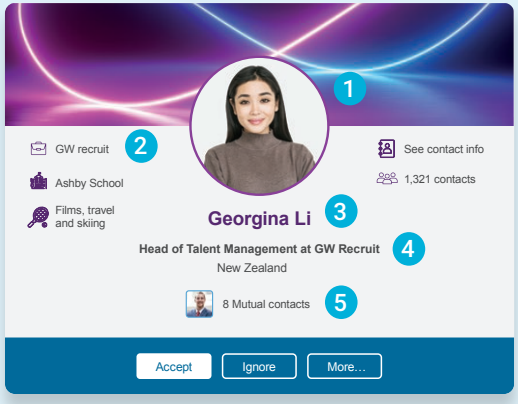
Malicious actors often aim to get to know you over the long term, so they can manipulate you into giving away sensitive information (willingly or unwittingly and sometimes in exchange for rewards).

Beware of fake employers or recruitment consultants.

Foreign state actors and criminals may pose as fake employers or recruitment consultants. They'll appear to present unique business or career opportunities. You may be asked for more details about yourself or your role.

- You could be tricked into sharing information without realising it's sensitive.
- You might think you're developing a legitimate business or career opportunity.

What does a malicious online profile look like?



A malicious approach through a fake profile will be framed in a way that appeals to you and your areas of interest. Watch out for these warning signs.

1 Profile picture

A picture of an attractive individual in a standard business setting such as an office.

2 Company description and affiliations

A description of a generic, non-descript consultancy or recruitment company with references to government contacts and state-owned enterprises.

3 Profile name

Typically, the profile name will be unfamiliar to you.

4 Unrealistic job roles

The person trying to lure you will often have a very senior job title even though their profile picture shows a young face.

5 Mutual contacts

Contacts with mutual friends may have been made to make the profile appear more legitimate. Many people do not fully check online profiles before accepting new requests.