Know the signs

Too good to be true
Offers remote, flexible working and a disproportionately high salary for the role advertised

Lack of depth or detail
Lacks any visible or checkable company information available online, and the role itself lacks tangible details

Flattery
Overly focuses on your skills or experience and refers to government or 'high-end' candidates

Urgency
Responds too quickly to messages, and attempts to rush you off the website onto another communication channel or platform

Scarcity
Emphasises so-called limited, one-off or exclusive opportunities

Imbalance
Disproportionately focuses on their company, rather than validating you as a possible candidate

What should you do?

- Review your account settings on social and professional networks to control the information that is available publicly, especially information relating to security clearances.
- Familiarise yourself with the guidance provided by your organisation and the relevant platforms you use.
- Form contacts online only with people you know or after having verified their identity as legitimate contacts.
- Report any contact from profiles you suspect are malicious, making sure to include in the report:
  - the URL of the profile
  - a screen shot of the message or request they sent
  - a brief explanation of why you think the approach is suspicious
  - any other relevant details.

Memorise the four Rs to protect yourself against malicious profiles:

Recognise
the profile?

Realise
the potential threat

Report
to your security manager/adviser

Remove
them from your network

For more information, talk to your security manager/adviser or visit:

www.asio.gov.au
www.cyber.gov.au

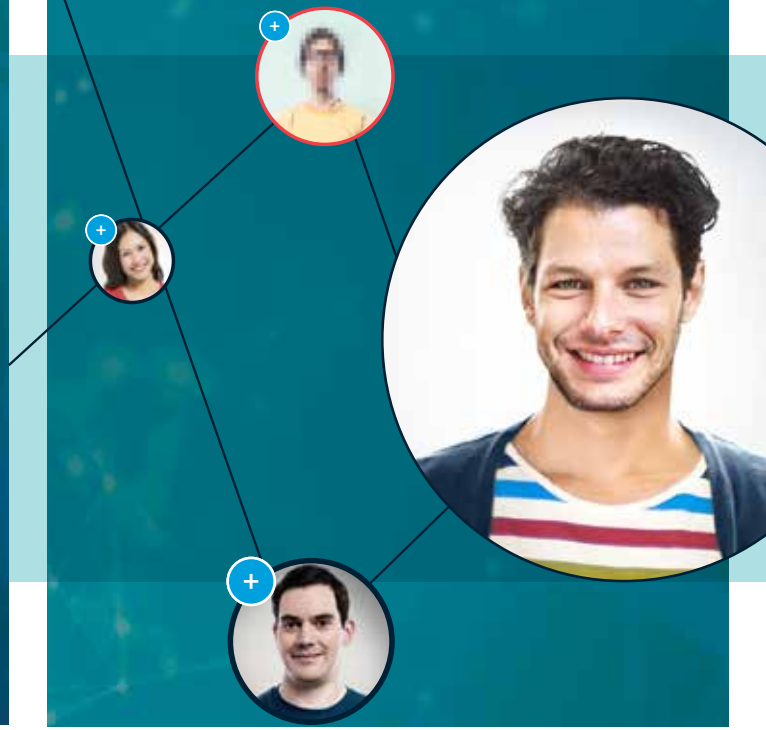
19-11034

Australian Government
Australian Security Intelligence Organisation

ASIO

Think before you link

Online networking guide



Have you ever encountered someone online who was not who they seemed?

Social and professional networking sites and other online platforms can be an extremely valuable tool for promoting yourself online and enhancing your career prospects, but they can also expose you to unforeseen risks.

‘This guide will help you to protect yourself, your colleagues, and your organisation from the harmful impact of malicious profiles online.’

The threat

What’s the problem?

Malicious actors use social and professional networking sites, email and other online platforms to target individuals with sensitive accesses.

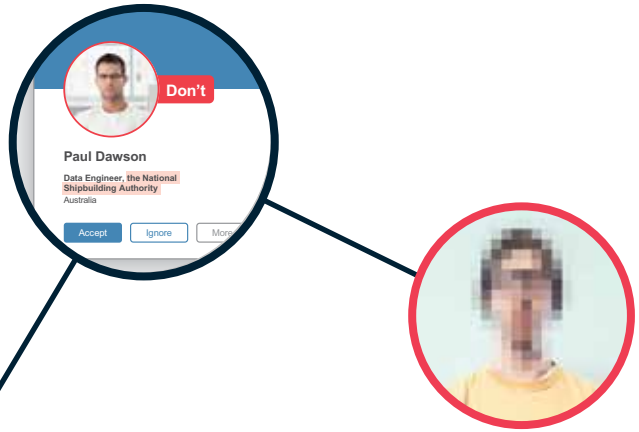
Why are they doing this?

- Their goal is to recruit Australian and Western nationals to provide them with sensitive information that is valuable to them.
- Loss of sensitive information could be harmful to you and your organisation, or pose a national security risk.

Who are they targeting?

You could be at greater risk of targeting if you:

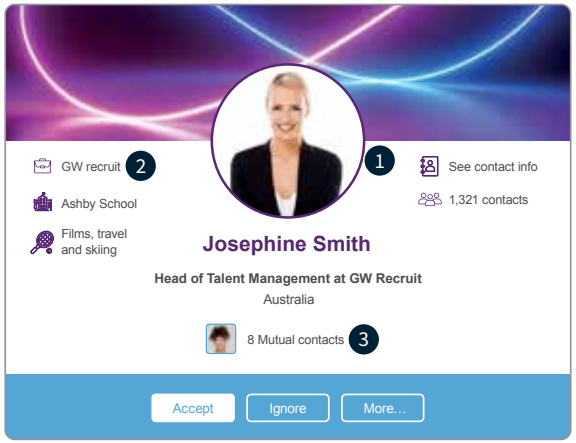
- publicly display that you work for the government, in the private sector or in academia with access to classified or commercially sensitive information, technology or research; or
- publicly disclose you have a security clearance.



How do they trick you?

- Malicious actors pose as fake ‘employers’ or recruitment consultants, appearing to present a unique business or career opportunity.
- They may ask for more details about your role, and try to learn about potential sensitive accesses you might have.
- Their aim is to build a longer term relationship and manipulate you into giving away sensitive information, willingly or unwittingly, sometimes in exchange for rewards.
- You may not realise the information you are sharing is sensitive and may believe the information you are providing is to develop a legitimate business or career opportunity.

What does a malicious profile look like?



1 Profile picture

It is often (but not always) a picture of a highly attractive individual in a formulaic business setting such as an office.

2 Company affiliation or description

This is often a generic, nondescript consultancy or recruitment company and refers to government contacts or state-owned enterprises.

3 Mutual contacts

Contacts with mutual friends may have been made to make the profile appear more legitimate. Many people don’t fully check the profiles of new requests.