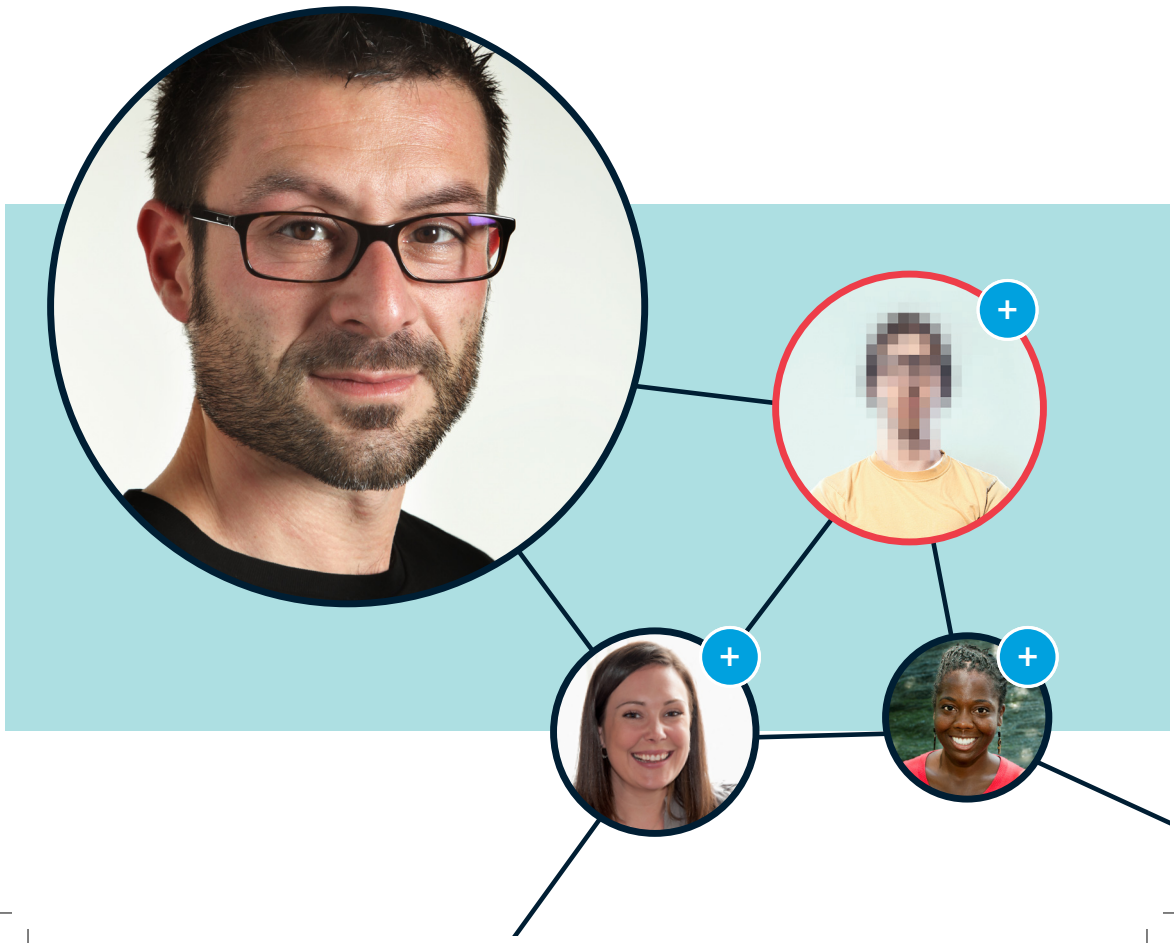
Australian Government

Australian Security Intelligence Organisation

ASIO

Think before you link

Online networking guide



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

In the digital age, online social and professional networking sites enable us to be more joined up than ever before, but they also expose us to unforeseen risks.

Introduction

Malicious actors behave anonymously or duplicitously online in an attempt to connect with people who have access to valuable and sensitive information. They often do this by posing as recruiters or talent agents, who approach you with enticing opportunities when their real intent is to gather as much information as possible from you. The consequences of engaging with these profiles can be damaging to your career, the interests of your organisation, and the interests of Australia's national security.

"This guidance will help you to protect yourself, your colleagues and your organisation from the harmful impact of malicious profiles. You'll know how to identify them, how to respond, and how to minimise the risk of being targeted in the first instance."

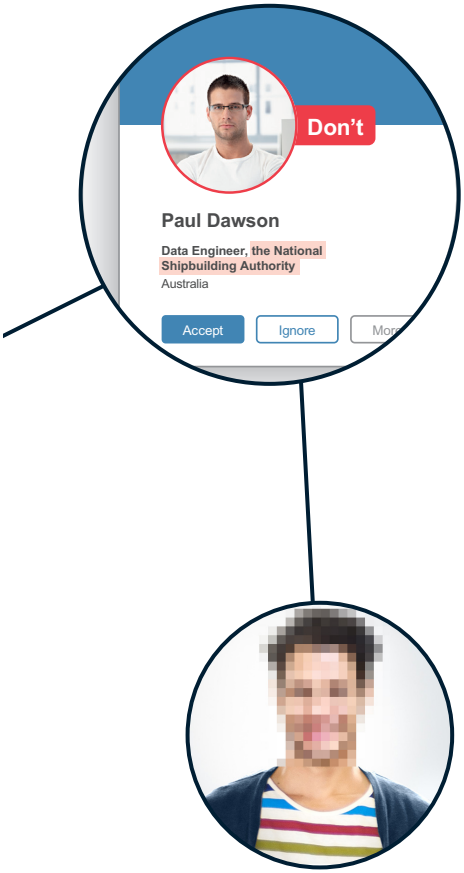
The threat

What's the problem?

Malicious actors are using email, social and professional networking sites, and social media platforms to approach Australian and Western nationals working in sensitive employment across government, the private sector, academia and think tanks.

Why are they doing this?

Their end goal is to recruit Australian and Western nationals who can provide them with sensitive intelligence, willingly or unwittingly. Individuals may not recognise that the information they are providing is sensitive (for example, they may be asked seemingly benign questions). Malicious actors piece together information from multiple sources to **draw meaning from their intelligence gathering.**



Who are they targeting?

Individuals are particularly vulnerable to approaches if they include the following details in their **profile**:

- identify as an employee of the **Australian Government**;
- identify as working in the private sector or academia, **with access to classified or commercially sensitive technology or research** either directly or indirectly (for example, the defence industry); or
- mention that they have a **security clearance**.

How do they trick you?

Typically, malicious actors contact the target posing as an interested 'employer' or recruitment consultant presenting **a unique business or career opportunity**. They ask for further details about the target's background, try to 'sell' the business opportunity, and insist on discussing it privately, away from the initial website or platform used to inititiate contact. This kind of engagement is an attempt to understand the level of access the individual has to sensitive information, draw it out from them, and build a longer term relationship. Most of the time the target is not aware of the real purpose of the approach. In some instances, they believe they are providing information to develop a legitimate business opportunity.

Memorise the four Rs to protect yourself against malicious profiles:

Recognise
the profile?

Realise
the potential threat

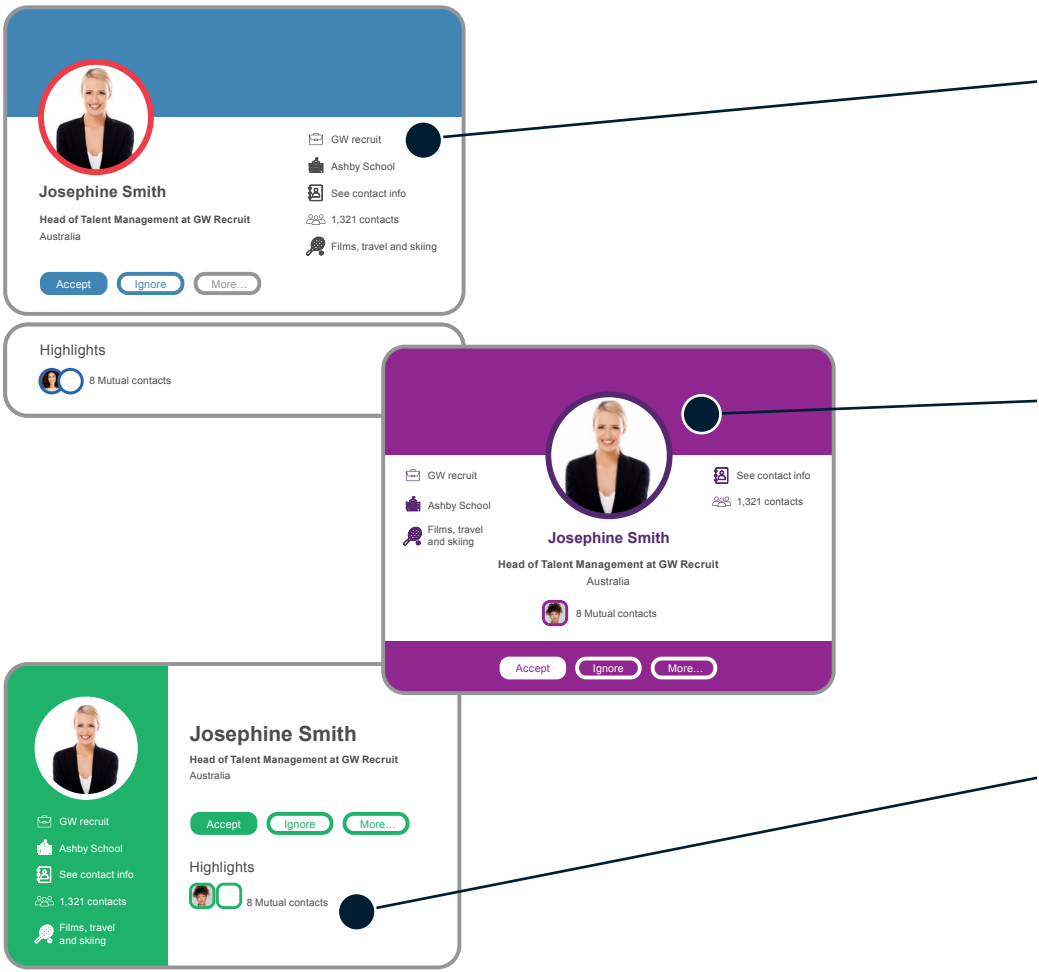
Report
to your security manager/adviser

Remove
them from your network

Recognise

the profile?

When a new connection adds you or gets in touch via email, social networks or other platforms, check to see if you recognise them first. If you do not recognise them, watch out for signs that may indicate fake or malicious profiles.


Josephine Smith
Head of Talent Management at GW Recruit
Australia
Accept
Ignore
More...
GW recruit
Ashby School
See contact info
1,321 contacts
Films, travel and skiing
Highlights
8 Mutual contacts
Josephine Smith
Head of Talent Management at GW Recruit
Australia
8 Mutual contacts
Accept
Ignore
More...
GW recruit
Ashby School
Films, travel and skiing
See contact info
1,321 contacts
Josephine Smith
Head of Talent Management at GW Recruit
Australia
Accept
Ignore
More...
Highlights
8 Mutual contacts
GW recruit
Ashby School
See contact info
1,321 contacts
Films, travel and skiing

Company affiliation or description

This is often a generic, nondescript consultancy or recruitment company, with references to government contacts or state-owned enterprises. It may contain content similar to other suspicious profiles.

Profile picture

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

Mutual contacts

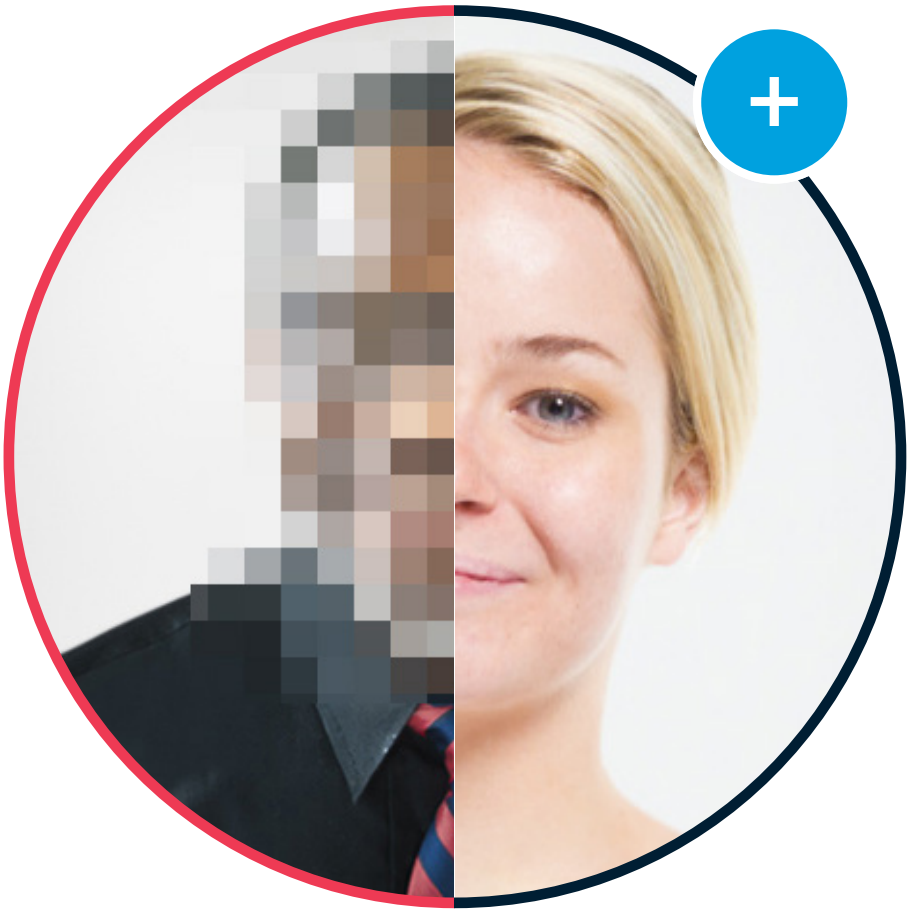
Contacts with mutual friends may have been made to make the profile appear more legitimate. Many people don't fully check the profiles of new requests before accepting.

What does a malicious profile look like?

Watch out for fake companies

We all know that things on the internet are not always as good as they seem. For example, when shopping online you might find what appears to be a great deal, but a quick look around the web can help you unmask a potential scam. The same is true of opportunities on social and professional networking sites. If you've been contacted by a profile or individual you don't recognise, consider the following:

- **Does the company have a web presence?** Usually, legitimate organisations will have multiple websites, or review sites, referring to them. There may be news articles or blog posts highlighting untrustworthy sites.
- If there is only one or a very small number of websites referring to the organisation, there's a good chance it is not real.
- If you can avoid it, do not proceed to the organisation's website—it may contain harmful material such as computer viruses.
- In an attempt to appear genuine, some malicious profiles have created cover websites, but these are often of low quality and do not have a lot of functionality.



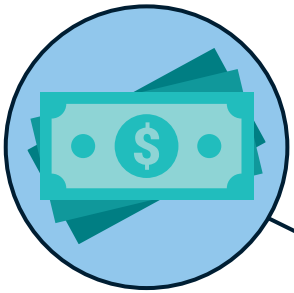
Realise

the potential threat

You may realise the threat from the way the profile looks and the kind of personal and professional information it lists. But, if not, the next signs you should look for are related to the way the profile engages with you.

Too good to be true

The profile, email or other communication offers remote, flexible working; a disproportionately high salary for the role advertised; or an invitation to write in a 'prestigious' journal or other publication—sometimes for a high fee. It may include an offer for thousands of dollars for writing a report or giving a presentation.



Lack of depth or detail

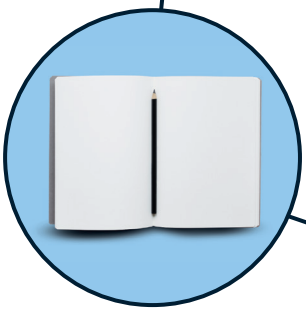
The information provided lacks details of any visible or checkable company information available online. The role itself lacks tangible details and instead focuses on working with unspecified clients.

Flattery

The information provided overly focuses on your skills or experience and refers to government or 'high-end' candidates.

Urgency

The profile is overly responsive to messages, and quick to secure a meeting. They attempt to rush you off the website or platform onto another communication channel or platform.



Scarcity

The information provided emphasises so-called limited, one-off or exclusive opportunities. It excessively uses terms like ‘high-end’, ‘high-impact’, ‘renowned’, ‘expert’ and ‘talent’.

Imbalance

The profile has a disproportionate focus on their company and the role being offered to you, rather than validating you as a possible candidate (for example, rarely or never asking for referees to verify your background).


SEARCH

What makes an approach suspicious?

Real versus fake: can you tell the difference?

Malicious profiles often pose as recruiters or talent agents, who approach you with enticing career opportunities. If you have never been approached by a talent agent before, it can be difficult to know whether an approach is genuine. There are some clear differences in the way real and fake recruiters operate; knowing the signs can help you tell the difference.

WARNING SIGNS

The following are very reliable signs that the person approaching you is not genuine:

- The candidate is asked to **pay any costs up front** and then be reimbursed in cash.
- The recruiter **fails to verify** the candidate's background (for example, not asking for further information such as references or transcripts).
- The candidate is asked to move onto **unusual online platforms** to communicate, and off the initial website or platform used to initiate contact.
- There are quick attempts to **set up a meeting abroad** rather than in Australia. Malicious profiles often want to progress the relationship at a rapid pace.

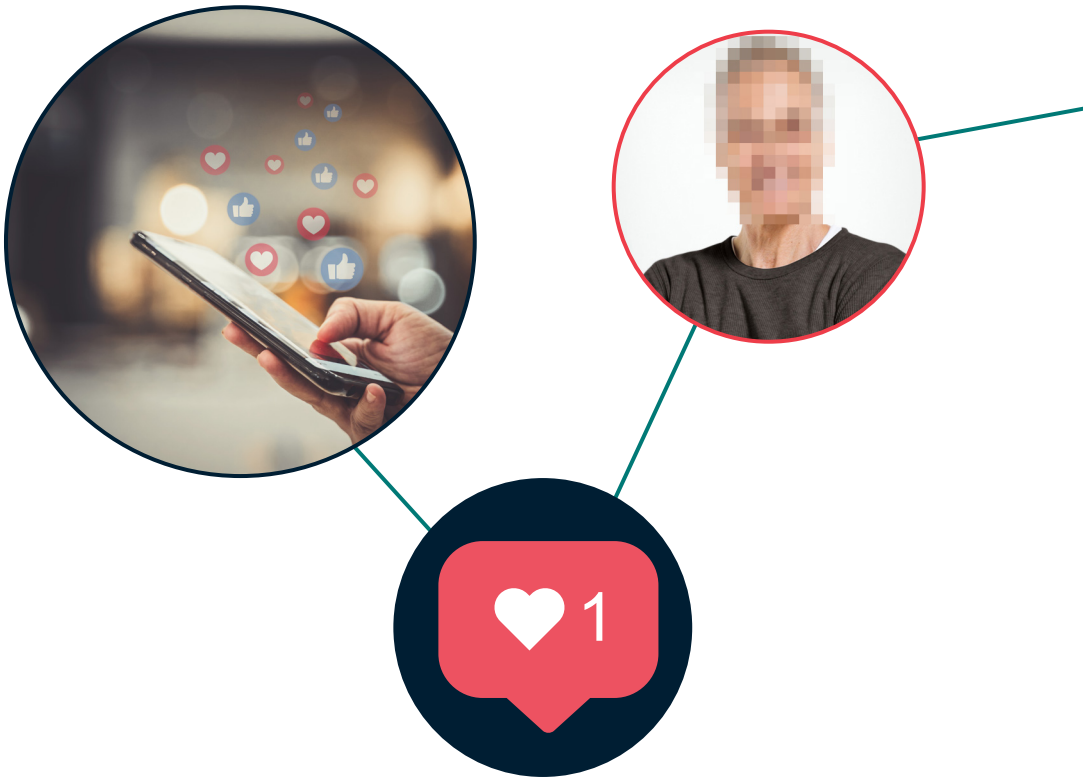
GOOD SIGNS

Not all recruiters operate in the same way, but if you spot several of these signs, there's a good chance the approach is genuine.

- The recruiter progresses at the **candidate's pace**, not the recruiter's—hurrying is a technique that malicious profiles use to encourage you to make poor judgements. Genuine recruiters will tend to let the potential candidate set the pace.
- The recruiter **validates** you as a candidate.For genuine head-hunters, this is a reciprocal process, during which time they also want to assess your suitability for the role (for example, asking for references).
- The recruiter attempts to **make life easier for the candidate**—for example, asking you to specify a convenient meeting time or location rather than deciding on one for you.
- **The recruiter manages the expectations** of the candidate. Real recruiters tend to be upfront about potential downsides of the role—it is important to them that you understand what is on offer.

Why do some people engage?

These online approaches work in a similar way to other ‘scams’ (for example, romantic, financial or cyber scams). It may be increasingly difficult to suspect the scam as it progresses, as you become psychologically invested and therefore reluctant to reassess your previous decisions. Many people may ignore their concerns and choose to focus on the so-called business opportunity.



Research suggests that scams target various susceptibilities relating to:

The message

Flattery—flattering you about your skills, experience et cetera

Authority—use of credible logos, overly 'glowing' reviews or a professional email signature, in an attempt to appear credible

Scarcity—framing it as a one-off, exclusive opportunity and rushing you to decide

The person

Appealing to your **identity** as a professional, and values such as being **valued, respected and rewarded**

The context

High workload and distractions, which are known to increase the chance of scam success

Recent job or life changes (for example, unemployment, or retirement)—these may be alluded to on your social media profile

Report

to your security manager/adviser

Once you realise that you might have been contacted by a malicious profile, reporting them to your agency's security manager/adviser is the best way to protect yourself and others.

When submitting a report to your security manager/adviser, make sure to include the following details:

- the URL of the profile (if approached through a website);
- a copy of the email or a screen shot of the message or request they sent;
- a brief explanation of why you think the approach is suspicious; and
- any other relevant details.

Ensure you disengage from the profile and don't interact any further.

Remove

them from your network

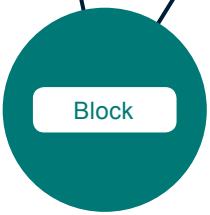
Keeping malicious profiles in your network adds legitimacy to them and puts your colleagues, organisation, and other contacts at risk.

Encourage your trusted friends and colleagues to also remove these profiles if they have connected too.

Remove the malicious profile from all your social media and social and professional networking sites.

It is important to remove suspected malicious profiles from your contacts because maintaining these contacts adds legitimacy to the profile and encourages other people to connect with them. Keeping these contacts puts others at risk.

It is also advisable to review your account settings. You should avoid settings or additional software that automates joining you up with new accounts, so that you aren't connected with accounts without your knowledge and permission.



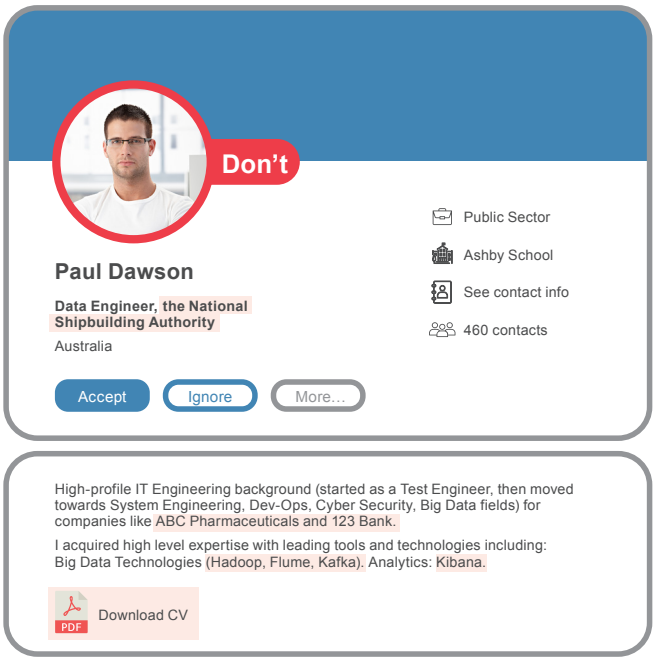
Many networking sites allow you to easily remove contacts just by accessing your directory and clicking on the relevant 'remove' or 'block' option for the malicious profile. Often you do not need to click on the profile itself to do this.

Final tips

Now you are aware of the risks of engaging with malicious profiles, how to recognise them and how to respond.

But there are some tips that can help you avoid being targeted in the first place.

Social and professional networking sites and other online platforms exist to help you promote yourself to potential employers, but if you are working in a sensitive area you have a responsibility to your organisation and your colleagues to protect yourself from the types of threats we've mentioned. Providing details about the nature of your work on publicly available sites makes you vulnerable to malicious targeting. The best way to stay safe online and reduce the likelihood of being targeted is to follow these dos and don'ts:



Don't

- advertise your security clearance publicly online;
- reveal details of sensitive job roles or employers publicly or to unknown contacts; or
- make all your profile information publicly available.

Do

- only once satisfied an approach is genuine, share sensitive details, such as a complete CV, or details of specific projects, over one-to-one trusted networks or in person with verified contacts;
- if necessary, include details of your security clearance in direct correspondence with genuine contacts;
- check your organisation's guidance and policy on the management of your digital footprint;
- use account settings to maintain your privacy and control who can view your profile (seek out the guidance on the relevant platforms you use); and
- take the time to find out and understand the profile settings available. The more personalised these settings are, the more control you have over your information.

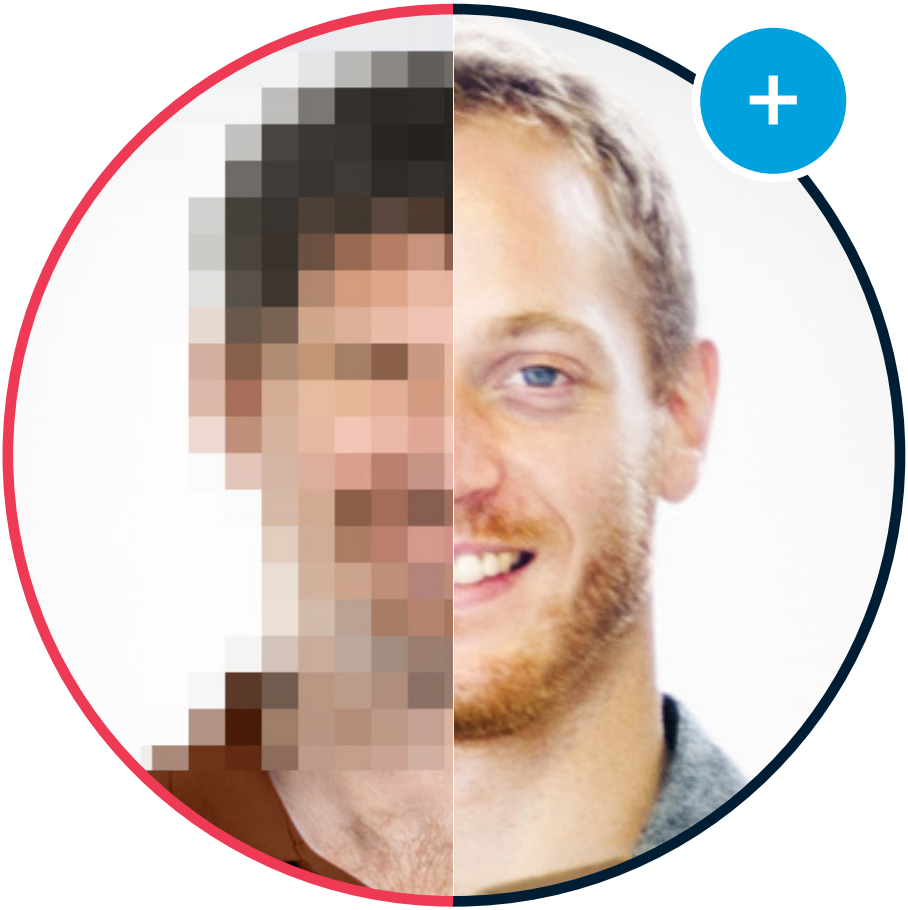
How should you network online safely?

Dealing with two audiences: the dual lens

Two audiences are potentially viewing your profile—genuine professional contacts who support your credibility and raise your profile, and those who want to exploit you and your organisation.

When managing your profile, provide enough relevant information to your genuine contacts without giving away so much detail that it makes you vulnerable to targeting by malicious profiles.

Think about the lowest level of detail that you need to provide for your profile to promote you properly to friendly audiences. What information is relevant to potential talent hunters or recruiters? Does your profile reveal unnecessary detail?



To protect yourself and your organisation from malicious profiles, start with making your online presence secure. And, when contacted by someone new, always remember the four Rs:

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

The information contained in this guide is general in nature. You should make your own judgement about the use of this document and seek independent professional advice on your particular circumstances. Organisations or individuals with questions about this advice can contact ASIO via our webiste.