



Australian Government

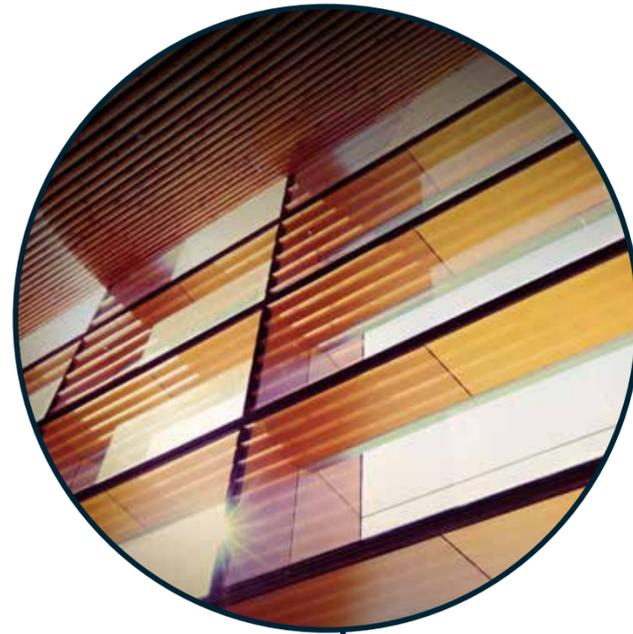
Australian Security Intelligence Organisation



Think before you link

Staff briefing pack





The threat

What?

Malicious actors using online platforms, apps, websites or emails to approach individuals



Why?

Recruitment of Australian and Western nationals to act as unwitting agents and provide them with sensitive intelligence



Who?

Those who:

- 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 (such as the defence industry); or
- mention that they have a security clearance.



How?

- Initially engages the individual online, presenting a 'unique' business offer
- Asks for further information about the individual and may request a CV
- Attempts to move the individual away from the initial website or other communication platform
- Sets up phone calls or face-to-face discussions
- May invite the individual to another country to meet a representative

Why is this relevant to you?

As a staff member with access to sensitive data, you are a desirable target for malicious profiles.

- Potential consequences of engaging with malicious actors can be serious (for example, loss of security clearance, funding or intellectual property).
- Our staff are vulnerable to attack.
- Campaign resources are designed to help you protect yourselves and your organisation from being manipulated.

Know the signs!



Countering the threat

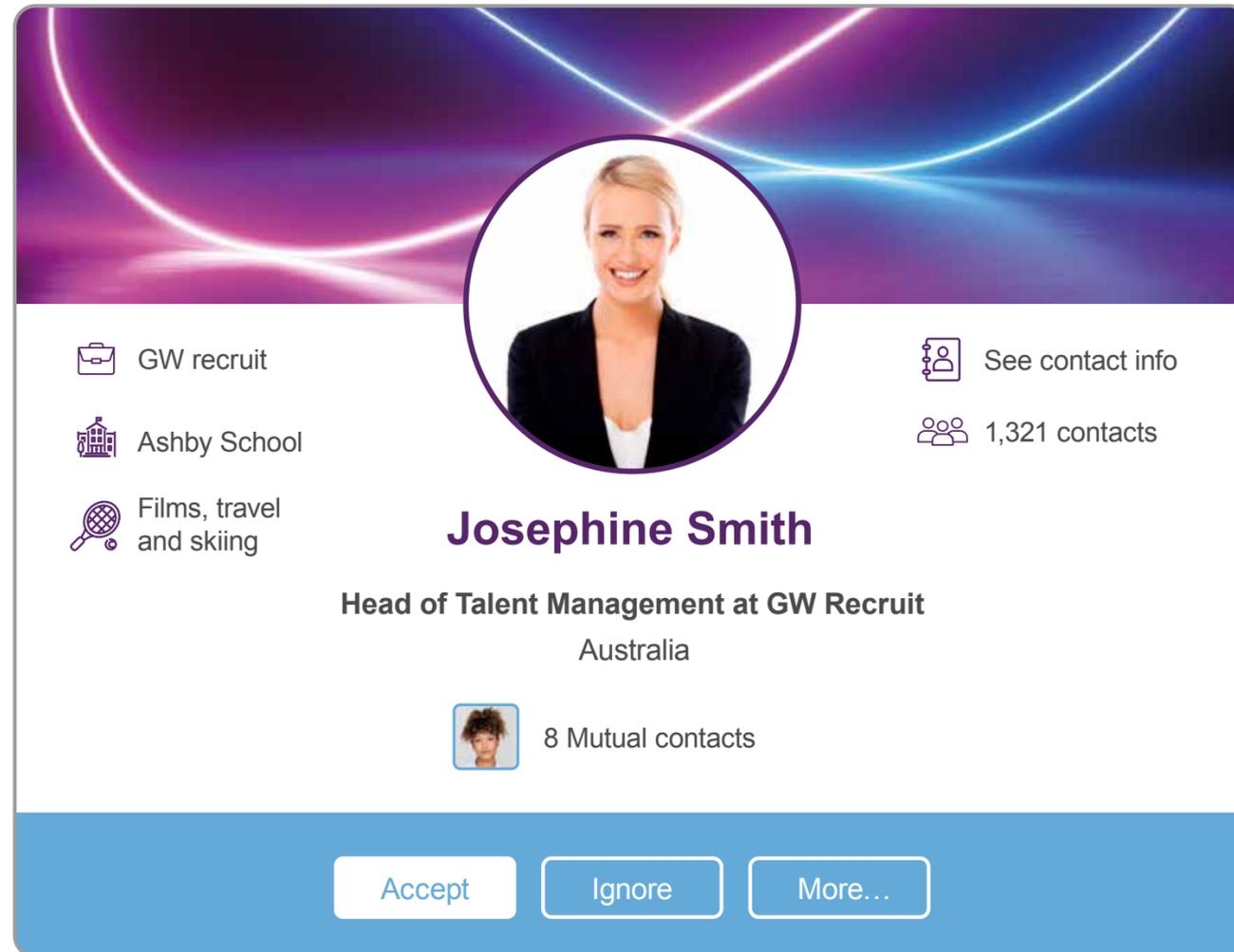
Recognise
the profile?

Realise
the potential threat

Report
to your security manager/adviser

Remove
them from your network

Recognise the profile?



A LinkedIn profile card for Josephine Smith. The card features a circular profile picture of a woman with blonde hair. To the left of the picture are three icons: a briefcase for 'GW recruit', a school building for 'Ashby School', and a magnifying glass for 'Films, travel and skiing'. To the right are two icons: a person with a plus sign for 'See contact info' and a group of people for '1,321 contacts'. Below the picture, the name 'Josephine Smith' is displayed in bold, followed by her title 'Head of Talent Management at GW Recruit' and location 'Australia'. At the bottom left, there is a small profile picture and the text '8 Mutual contacts'. At the bottom of the card, there are three buttons: 'Accept', 'Ignore', and 'More...'. The background of the card has a purple and blue abstract design.

GW recruit

Ashby School

Films, travel and skiing

See contact info

1,321 contacts

Josephine Smith

Head of Talent Management at GW Recruit

Australia

8 Mutual contacts

Accept Ignore More...



Realise the threat

Genuine recruitment approaches

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

- progresses at the candidate's pace, not the recruiter's;
- validates you as a candidate;
- attempts to make life easier for the candidate; and
- manages the expectations of the candidate.

Realise the threat?

Illegitimate recruitment approaches

These are very reliable signs that the person approaching you is not genuine.



Too good to be true



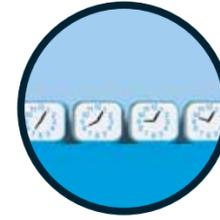
Lack of depth or detail



Flattery



Imbalance



Urgency



Invitation to a foreign country



Scarcity of opportunity

Personal vulnerabilities which they can exploit include:

- high workload and distractions;
- recent job or life changes (for example, unemployment or retirement); and
- your identity as a professional, and values such as being valued, respected and rewarded which they may appeal to.

Report to your security manager/adviser

- Do not engage.
- Report to your security manager/adviser or line manager, and 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/request they sent
 - other relevant details
 - signs that made you suspect the profile was malicious.
- Do not engage any further with the profile.
- Be assured this matter will be treated with discretion and taken seriously.



Remove them from your network

The image shows a LinkedIn profile card for Josephine Smith. The card has a purple and blue gradient header with a circular profile picture of a woman. Below the picture, the name 'Josephine Smith' is displayed in bold purple text, followed by her title 'Head of Talent Management at GW Recruit' and location 'Australia'. To the left of the name are three icons representing her affiliations: 'GW recruit' (briefcase), 'Ashby School' (school building), and 'Films, travel and skiing' (globe). To the right are two icons: 'See contact info' (person with ID card) and '1,321 contacts' (group of people). Below the name, there is a small profile picture of another person and the text '8 Mutual contacts'. At the bottom of the card, there is a blue bar with three white buttons: 'Accept', 'Ignore', and '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

8 Mutual contacts

Accept Ignore More...

Take-away messages

You can avoid making yourself a target online by:

- not advertising your security clearance publicly online;
- not revealing details of sensitive job roles or employers publicly or to unknown contacts;
- thinking about the lowest level of detail that you really need to include on your profile;
- using website settings to manage the information you put out about yourself, and to control who can view your profile; and
- sharing CVs or details of specific projects only with trusted and verified contacts.



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

www.asio.gov.au

www.cyber.gov.au

Any questions?

