FOLD

FOLD

Memorise the four Rs to protect yourself against malicious profiles:

R ecognise
the profile?

R ealise
the potential threat

R eport
to your Security Manager

R emove
them from your network

Know the signs

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

Lack of depth/detail
A lack of any visible or checkable company information available online. The role itself lacks tangible details.

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

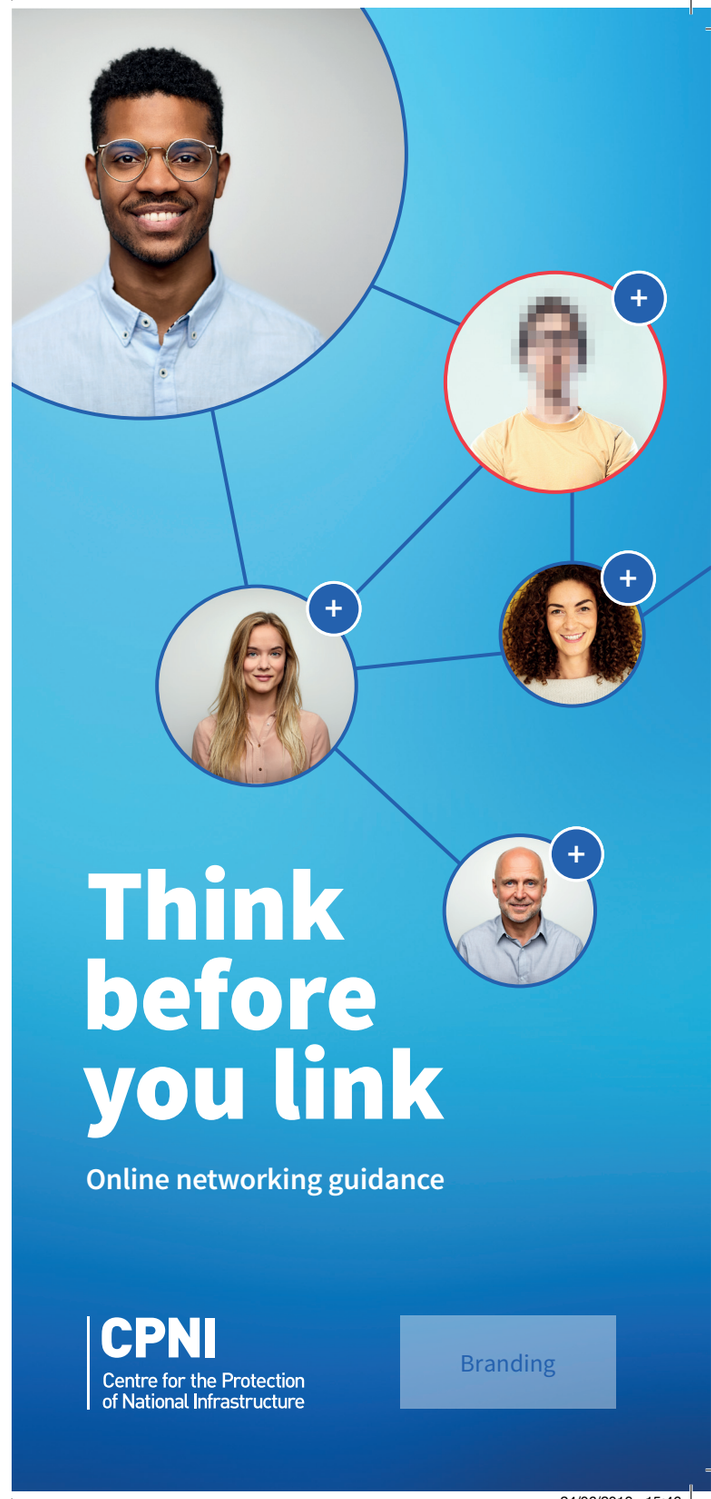
Urgency
Overly responsive to messages. Attempts to rush you off the website onto another communication method.

Scarcity
Emphasis on so called limited, one-off or exclusive opportunities.

Imbalance
Disproportionate focus 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 relating to security clearances
- Familiarise yourself with the existing guidance provided by your organisation and the relevant platforms you use
- Only form contacts online with people you know or after having verified their identity as legitimate contacts
- Report any contact from profiles you suspect are malicious



Think before you link

Online networking guidance

CPNI
Centre for the Protection of National Infrastructure

Branding

FOLD

FOLD

FOLD

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

Social and professional networking sites can be a hugely valuable tool for promoting yourself online and enhancing your career prospects but can also expose you to unforeseen risks.

“This guidance 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?

Hostile actors and **criminals** use social and professional networking sites to target individuals with sensitive accesses

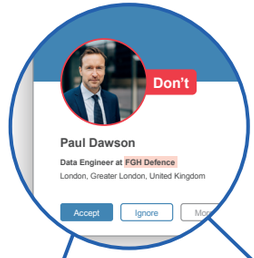
Why are they doing this?

- Their end goal is to recruit UK 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:

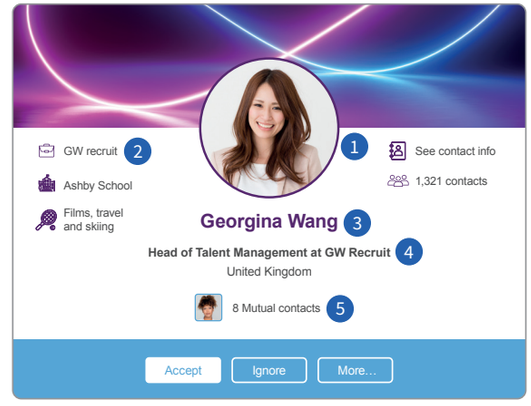
- Publicly display that you work for the government, or in the private sector with access to classified or commercially sensitive information, technology or research
- Publicly disclose your UK security cleared or developed vetting security clearance if you hold one



How do they trick you?

- Hostile actors and criminals 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 access 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
- The target may not realise the information they are sharing is sensitive and may believe the information they are providing is to develop a legitimate business or career opportunity

What does a malicious profile look like?



1 Profile picture

Picture of highly attractive individual in a formulaic business setting such as an office.

2 Company affiliation/description

Generic, non-descript consultancy or recruitment company. Reference to government contacts, ‘state owned’ enterprises.

3 Profile name

Typically this is a common western first name followed by a foreign surname.

4 Unrealistic job roles

Very senior or high-profile job roles, with a young profile picture.

5 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.

FOLD