# Think before you link

## A guide to networking safely online

PSR | Protective Security Requirements

## Have you ever encountered someone online who was unusually interested in you and your work?

Professional and social networking sites are useful tools in the digital age but they can also expose you to unforeseen risks.

# About this guide

Criminals and foreign state actors use anonymous or fake online profiles to try and connect with people who have access to valuable or sensitive information and resources. They'll often pose as recruiters or talent agents, and may approach you with enticing opportunities. Falling for these tactics could damage your career and your organisation – you could even be compromising national security.

**This guide will help you to protect yourself, your colleagues, and your organisation from the harmful impact of malicious online profiles. You'll learn how to identify and respond to a suspicious approach, and how to minimise the risk of becoming a target in the first place.**

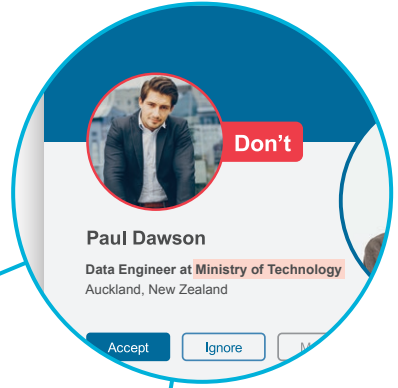
# Understand the threat

## What is the threat?

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

## What are their motives?

People who use malicious online profiles aim to exploit their targets for criminal, social, economic, or political gain. Because it's easier to disguise their true identity and intentions online, this kind of deception is a useful tool for foreign state actors and criminals alike. Their goal is to recruit targets and get them to provide sensitive or valuable information.




## Who do they target?

Malicious actors look for people with high status positions who may have access to valuable information or resources.

Your people are at greater risk of being targeted if they:

- disclose that they have access to classified or commercially-sensitive information, technology, or research
- reveal they have a national security clearance.

## How do they trick their targets?

Malicious actors often appeal to their target using flattery or by offering something valuable. They'll then try to build rapport with their target. Developing a long-term relationship gives them more opportunity to manipulate their target into giving away sensitive information (willingly or unwittingly, and sometimes in exchange for rewards).

Foreign state actors and criminals often pose as employers or recruitment consultants. They'll try to present their target with a unique business or career opportunity. Under this guise, they may ask for more details such as their exact role within your organization as they try to find out if they have access to sensitive information. The target may not realise the information they share is sensitive and just feel that they are responding to a legitimate business or career opportunity.

# Remember the four Rs to protect yourself against malicious profiles:

**Recognise**
a suspicious profile

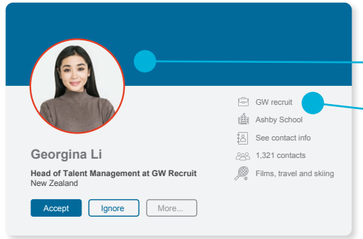
**Realise**
the potential threat

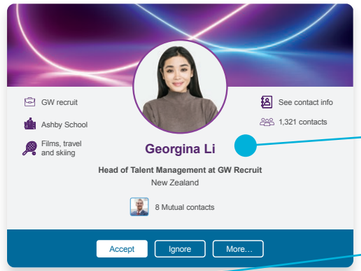
**Report**
your concerns

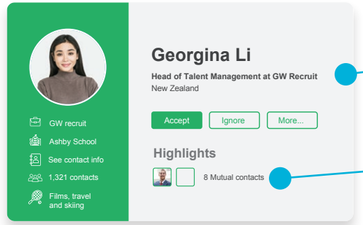
**Remove**
them from your network

# Recognise a suspicious profile

When a new contact adds you or gets in touch on a social or professional networking site, check to see if you recognise them first. If you don't recognise them, look for signs of a malicious profile.




## Profile picture

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

## Company description and affiliation

The description of the consultancy or recruitment company is generic, non-descript and includes references to government contacts and state-owned enterprises.

## Profile name

Typically, the profile name will be unfamiliar to you.

## Unrealistic job roles

The job role will usually be very senior or high-profile (even though the profile picture shows a young face).

## Mutual contacts

The profile may show contacts with mutual friends to make the profile appear more legitimate. Remember that many people do not fully check online profiles before accepting new requests.

# What does a malicious profile look like?

## Watch out for fake companies

We've all come across websites that seem suspicious, and even though you may not fully understand why, further investigation may help you to uncover a potential scam. The same is true of online networking. If you've been contacted by someone with a profile you don't recognise, take a closer look!


### What to look for

- Does the company have a web presence? Usually legitimate organisations will have multiple websites or review sites referring to them. If there are limited references to the organisation, there's a chance it's not real.
- Before you proceed to the company's website, search for news articles or blog posts highlighting untrustworthy sites. You might find the fake company is listed.
- If you can avoid it, don't visit the organisation's website, as it may contain harmful material such as malware and viruses.
- In an attempt to appear genuine, some people with malicious profiles create cover websites, but these are often of low quality and don't have a lot of functionality.
- Err on the side of caution if it doesn't feel right or seems suspicious. Only proceed if you can prove the company is legitimate or avoid it altogether.

# Realise the potential threat

How a profile appears and the kind of personal and professional information it lists may raise your suspicions. Here are some warning signs to look out for if you're approached online by someone you don't know.

## It's too good to be true

You may be approached in a way that appeals to your areas of interest. You could be offered remote, flexible working and a disproportionately high salary for the role advertised. You might get an invitation to write in a 'prestigious' publication or to deliver a paid presentation. Or you might be offered a lucrative consultancy role in your area of expertise.

Like the old saying goes, if it looks too good to be true, then it probably is!

## The information lacks depth and detail

The online information about the company will usually lack depth and detail, making it harder to check and verify. The role on offer will also lack tangible details and instead focus on working with unspecified clients.

## Flattery is involved

The approach will often be overly focused on your skills and experience, and include a reference to government or 'high-end' candidates. Terms like 'high-end', 'high-impact', 'renowned', 'expert', and 'talent' are often used excessively.

## Urgency is a hallmark of the contact

Tactics involving urgency are used, such as being overly responsive to messages, being quick to secure a meeting, and attempting to rush you off the website or platform onto another communication method.


## Exclusivity is used as a lure

The emphasis is on the offer or opportunity being 'limited', 'one-off' or 'exclusive'. You only have short amount of time to take up the opportunity.

## The information lacks balance

The focus is mostly on their company and the role being offered to you — they're not focused on validating you as a possible candidate (they rarely or never ask for references to verify your background).

# What makes an approach suspicious?

People with malicious profiles often pose as recruiters or talent agents who present you with enticing career opportunities.

If you've never been approached by or engaged with an agent before, it can be difficult to know whether the approach is genuine. However, there are some clear differences in the way real and fake recruiters operate; knowing the signs can help you to spot when an approach is fake.

## Real versus fake: can you tell the difference?

"You may sometimes become aware of an opportunity through unconventional means, but if the opportunity is genuine, the process that helps you to realise it will also be genuine."

### WARNING SIGNS

If it doesn't feel right, then it probably isn't. You should be suspicious if the recruiter or agent:

- asks you to pay any up-front costs, with the promise of being reimbursed (in cash) at a later date
- makes no attempt to verify your background, experience, or credentials by asking for references or evidence of qualifications
- shows a lack of protocol — legitimate recruitment work is usually administered through a company's human resources team, and they'll have clear and credible processes
- asks you to move to another or unusual online platform to communicate, away from the initial means of contact
- uses unusual email addresses and phone numbers
- makes quick attempts to set up a meeting, possibly overseas (they try to progress the relationship at a rapid pace)
- talks about unusual or unclear incentives with an emphasis on high financial rewards
- has to provide you with reassurances that they're legitimate.

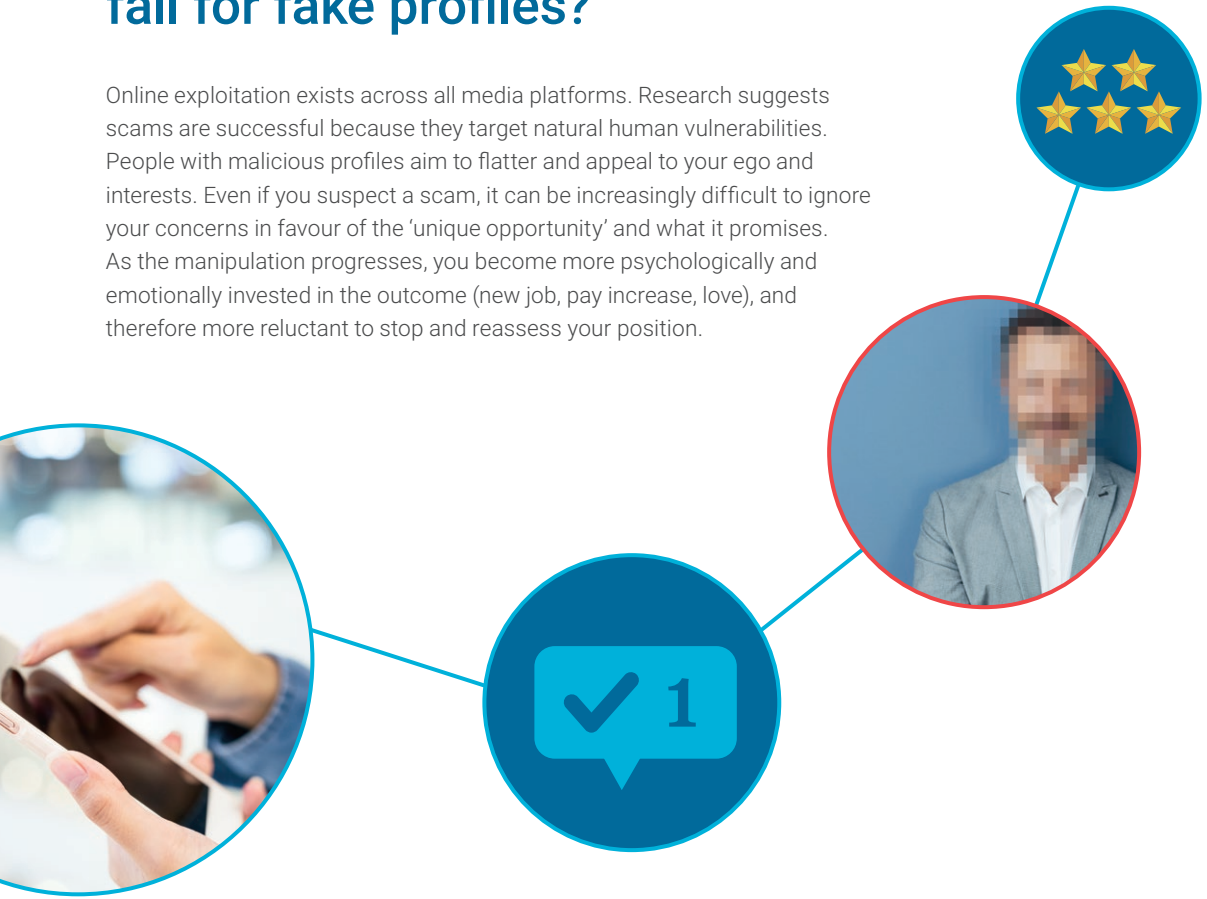
### GOOD SIGNS

Not all recruiters operate in the same way, but an approach is more likely genuine if the following signs are present.

- You can verify the identity of the recruiter, the recruitment agency, and the employer.
- Progress is at your pace, not the recruiters. Hurrying is a technique that malicious actors use to put you under pressure and encourage poor judgement. For example, they may impose time restraints to increase the sense of urgency and emphasise 'one-time offer' opportunities, so you rush your decision.
- The recruiter seeks to validate you as a candidate. For genuine headhunters, this process is reciprocal. They'll also want to establish your suitability for the role (for example, by asking for references).
- You're given a choice about meeting at times and in places that are convenient for you, rather than them deciding for you or giving you no choice at all.
- The recruiter manages your expectations about the role. Genuine recruiters tend to be upfront about the potential downsides of a role; it's important to them that you understand what's on offer.

# Why do some people fall for fake profiles?

Online exploitation exists across all media platforms. Research suggests scams are successful because they target natural human vulnerabilities. People with malicious profiles aim to flatter and appeal to your ego and interests. Even if you suspect a scam, it can be increasingly difficult to ignore your concerns in favour of the 'unique opportunity' and what it promises. As the manipulation progresses, you become more psychologically and emotionally invested in the outcome (new job, pay increase, love), and therefore more reluctant to stop and reassess your position.



# Like a trojan horse, how you can be manipulated is hidden in:

### The content of the message

**Flattery** – Does the message flatter your skills, experience, and potential?

**Authority** – Does the message attempt to appear credible by using official logos, branding, and a professional email signature? Does it also include overly glowing reviews from cover websites?

**Exclusivity** – Is the opportunity in the message framed as an exclusive one-off with time constraints, so you have to rush your decision?

### Your self-perception

Using your own ego against you, malicious actors will appeal to your identity as a professional and your desire to be valued, respected, recognised, and rewarded.

### Your current situation

High workload and distractions are known to increase the chance of a scam's success, as people typically make worse decisions when they're under pressure.

You'll be more susceptible to manipulation if you're vulnerable and anxious, particularly if you've experienced recent life changes like unemployment or bereavement. Your social media profile may even mention these life changes. An approach may come in the form of intimidation and could lead to blackmail.

"If you think you may be vulnerable to any form of exploitation, seek guidance from your security team."

# Report your concerns

Your organisation will have a way for you to report suspicious online profiles, approaches, and content. It's best to use established channels and approved processes to report what you encounter. If you're not sure how or where to report your concerns, ask your manager or security team for guidance.

## Disengage first, then report

If you suspect you've encountered a malicious profile, disengage from the profile; do not interact any further. Then you must report the encounter to your security team or line manager. Give them the following details:

- the URL of the profile
- a screen shot of the message or request you received
- a brief explanation of why you think the approach is suspicious
- any other relevant details.

## Contact the social or professional networking company when instructed to

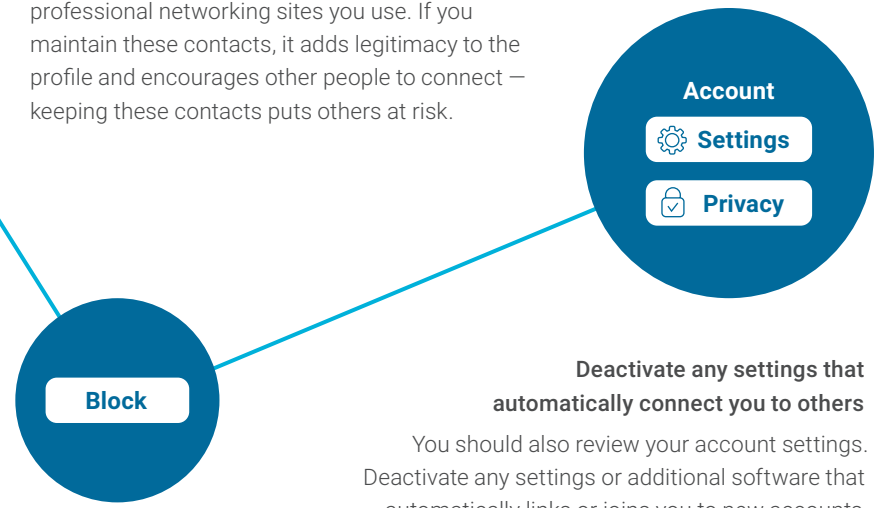
It's also important to report malicious activity to the platform provider. When instructed by your security team or line manager, report the malicious activity to the relevant social or professional networking company. Each company will offer detailed advice on how to manage and report malicious profiles experienced through their platforms.

# Remove them from your network

Maintaining malicious profiles in your network adds to their legitimacy, enhances their effect, and exposes your colleagues and organisation to further exploitation.

## Remove the malicious profile from every networking site you use

It's important to remove suspected malicious profiles immediately from any social or professional networking sites you use. If you maintain these contacts, it adds legitimacy to the profile and encourages other people to connect — keeping these contacts puts others at risk.




Many networking sites allow you to remove contacts by accessing your directory and clicking on the relevant remove or block option. You often don't need to click on the profile itself to do this.

**Deactivate any settings that automatically connect you to others**

You should also review your account settings. Deactivate any settings or additional software that automatically links or joins you to new accounts. If automatic settings are enabled, you can't check and verify whether an approach is legitimate, which raises your risk of being targeted.

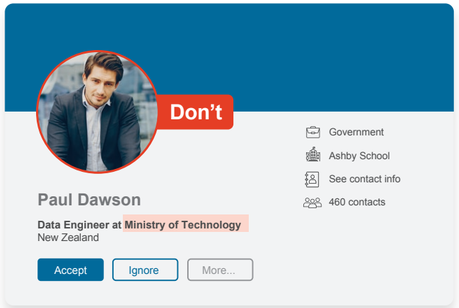
# Final tips

Now you're aware of the risks, here are some steps you can take to avoid being targeted.

You can keep using social and professional networking sites to help you connect with potential employers and generate new opportunities. However, you must take care with how you present yourself.

If you're working in a sensitive area, or have privileged access to valuable resources, you have a responsibility to your organisation and colleagues to protect yourself and them against the threats posed by malicious online profiles.

Publicly providing details about the nature of your work and your access privileges on social media and professional networking sites exposes you to scrutiny, and increases your risk of becoming a target of exploitation attempts.



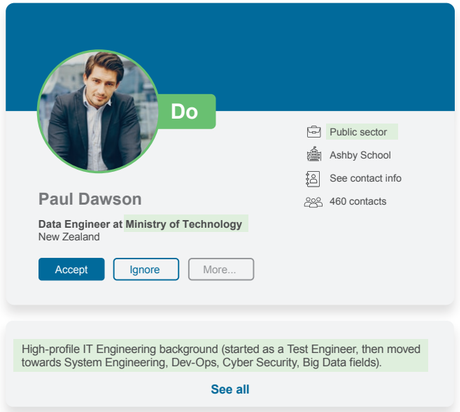

"The internet is full of dark alleyways, don't wander down them!"

**Don't**

- Disclose that you have access to classified or commercially-sensitive information, technology, or research
- Publicly disclose that you have a national security clearance
- Reveal details of sensitive job roles and projects to potential employers or unknown contacts
- Make all your profile information publicly available
- Disclose any information to any person, over any means, when you cannot validate their identity

**Do**

- Follow the security advice provided by your organisation
- Check your media settings, and keep patching and security software up to date
- Only share sensitive details, such as a complete CV or details of specific projects, to approved individuals using authorised communication channels and in the correct physical security environment
- Check your organisation's guidance and policy on managing your digital footprint
- Use account settings to maintain your privacy and control who can view your profile (each platform you use will have guidance about doing this)
- Take the time to learn what profile settings are available — the more personalised these settings are, the more control you'll have over your information
- Report any suspicions you have



# How should you network online safely?

## The dual lens: dealing with two audiences

Two main types of audience may view your online profile:

1. Genuine professional contacts who support your credibility and raise your profile.
2. People who may seek to exploit you, based on the information you reveal about yourself.

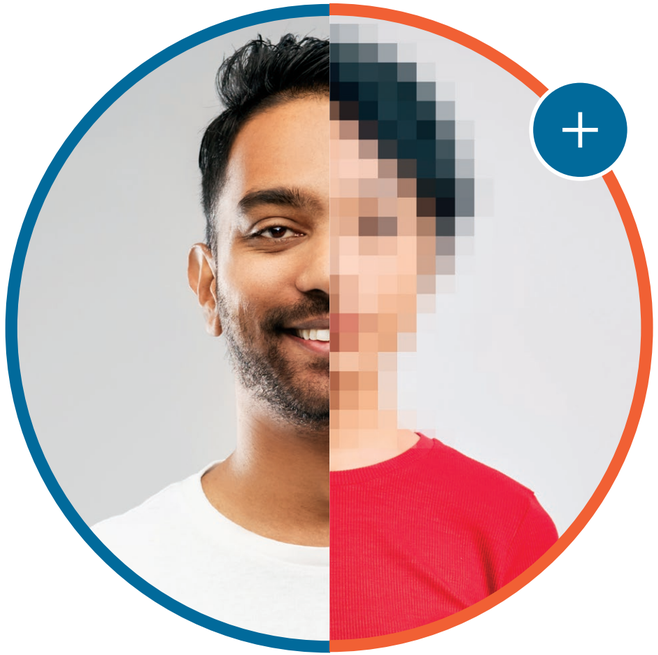
### Think of your profile like a shop window

Use your online profile for providing a summary of yourself — a shop window of sorts. Aim to provide an impression of what you may have to offer, rather than a full disclosure of everything you know and have done.

### Remove unnecessary details

Provide only the minimum level of relevant information you require to promote yourself properly to friendly audiences, talent hunters, or recruiters.

Tailor the information you provide to the audience you would like to attract, but don't give away so much detail that it makes you vulnerable to being targeted.



Start making your online presence secure so you can protect yourself and your organisation from malicious profiles. And, when contacted by someone new, always remember the four Rs:

**Recognise**
a suspicious profile?

**Realise**
the potential threat

**Report**
your concerns

**Remove**
them from your network

# PSR | Protective Security Requirements

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