Think before you link

Online networking guidance

CPNI
Centre for the Protection of National Infrastructure

Branding

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

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

Introduction

Criminals and hostile actors may act 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 will 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 UK national security and prosperity.

> **“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”**

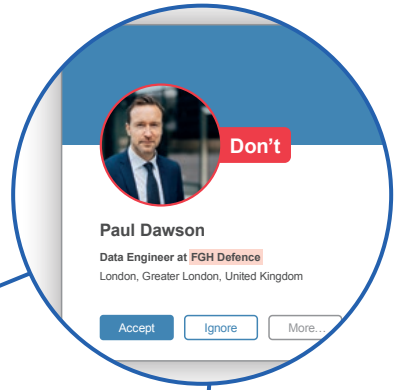
The threat

What's the problem?

Hostile actors and **criminals** are known to be using social and professional networking sites and social media platforms to approach UK 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 UK and Western nationals to provide them with sensitive intelligence, willingly or unwittingly. In these cases, individuals may not recognise that the information they are providing is sensitive (e.g. 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 on their profile:

- Identifying as an employee or member of **HMG or Civil Service**
- Identifying as working in the private sector or academia, **with access to classified or commercially sensitive technology or research** either directly or indirectly (e.g. the defence industry)
- Mentioning that they have **security clearances**, especially security cleared (SC) or developed vetting (DV)

How do they trick you?

Typically, hostile actors and criminals contact the target posing as an interested 'employer' or recruitment consultant presenting **a unique business 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. 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:

R ecognise
the profile?

R ealise
the potential threat

R eport
to your Security Manager

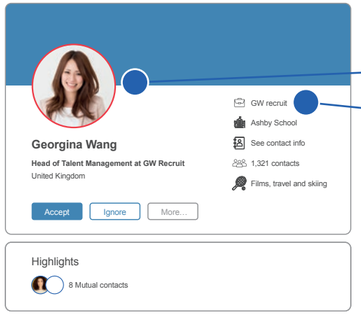
R emove
them from your network

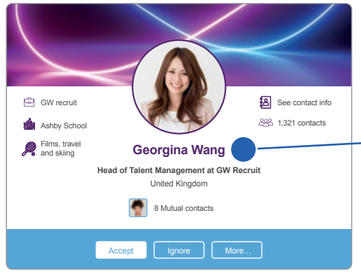
Recognise

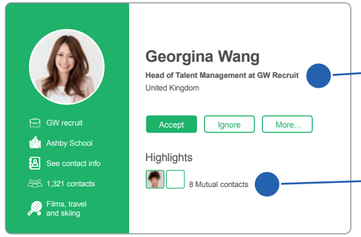
the profile?

When a new connection adds you or gets in touch on social networks check to see if you recognise them first.

If you do not recognise them watch out for signs that you can associate with fake or malicious profiles.







Profile picture

Picture of highly attractive individual in a formulaic business setting such as an office. Largely detectable with reverse image search.

Company affiliation/description

Generic, non-descript consultancy or recruitment company. Reference to government contacts, ‘state owned’ enterprises. Similar content to other suspicious profiles.

Profile name

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

Unrealistic job roles

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

Mutual contacts

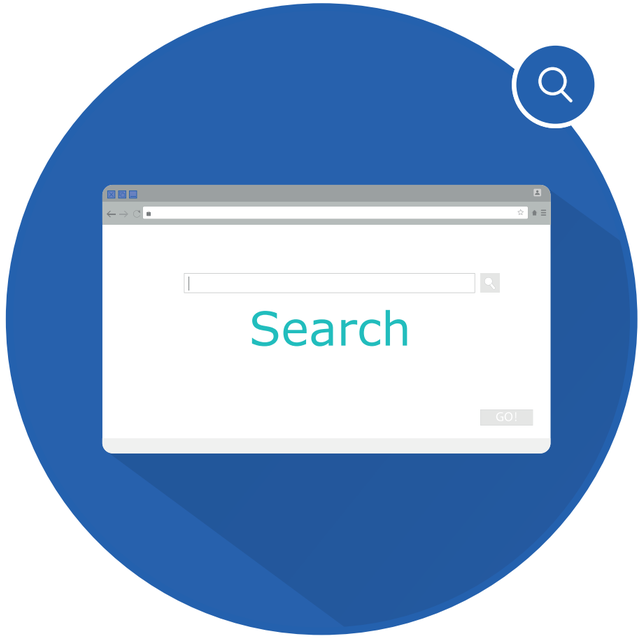
Contacts with mutual friends may have been made to make the profile appear more legitimate. Many people don’t fully check the profiles of new requests before accepting.

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 looks like 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 you don't recognise…

- **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

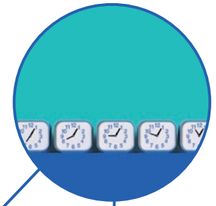
Offering remote, flexible working, a disproportionately high salary for the role advertised, an invitation to write in a 'prestigious' journal or other publication – sometimes for a high fee. This may be an offer for thousands of pounds for writing a report or giving a presentation.

Lack of depth/detail

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

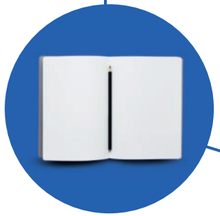
Flattery

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



Urgency

Overly responsive to messages, and quick to secure a meeting. Attempts to rush you off the website/platform onto another communication method.



Scarcity

Emphasis on so called limited, one-off or exclusive opportunities. Excessive use of terms like "high-end", "high-impact", "renowned", "expert", "talent".

Imbalance

Disproportionate focus on their company and the role being offered to you, rather than validating you as a possible candidate (e.g. rarely or never asking for referees to verify your background).

What makes an approach suspicious?

Real vs. 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

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

- Candidate being asked to pay any costs up front and then being reimbursed in cash
- If the recruiter **fails to verify** the candidates background (e.g. asking for further information such as references or transcripts etc.)
- Asks the candidate to move onto **unusual online platforms** to communicate, and off the initial website.
- Quick attempts to set up a meeting abroad rather than the UK or the home country. Malicious profiles often want to progress the relationship at a rapid pace.

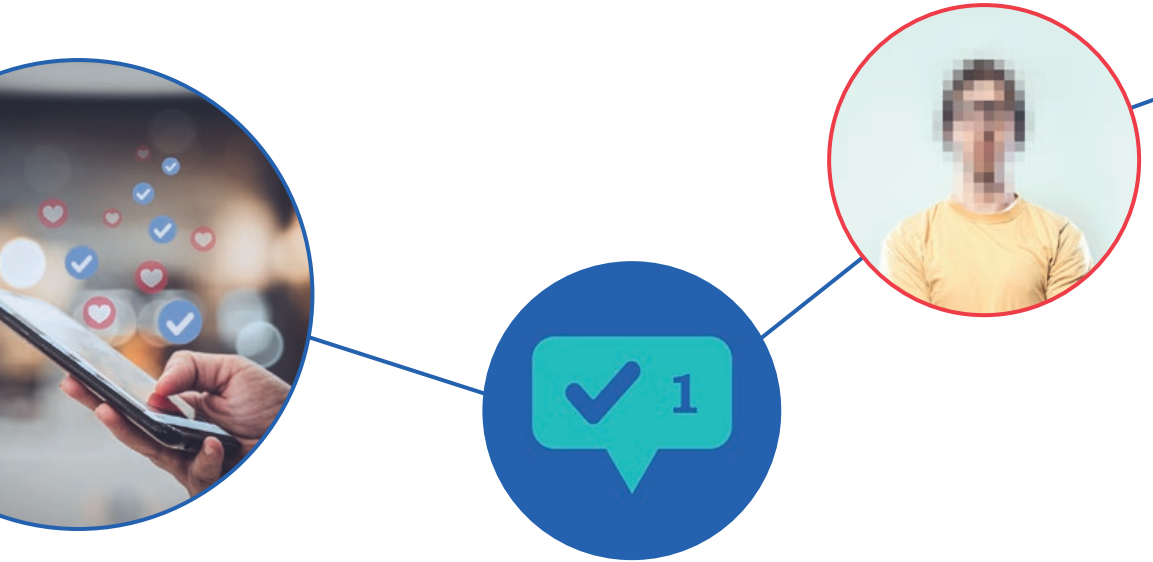
GOOD SIGNS

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

- Progress at the **candidate's pace**, not the recruiters – 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.
- **Validate** 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 (e.g. asking for references).
- Attempt 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.
- **Manage 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’ (e.g. romance, financial, 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 your skills, experience etc.

Authority – use of credible logos, overly ‘glowing’ reviews, professional email signature, in an attempt to appear credible

Scarcity – framing this 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, rewarded etc.**

The context

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

Recent job or life changes (e.g. unemployment, retirement) – these may be alluded to on your social media profile

Report

to your Security Manager

Once you realise that you might have been contacted by a malicious profile, reporting them to your Security Manager is the best way to protect yourself and others.

All platforms provide robust reporting mechanisms for suspicious profiles or content and you should report through these channels as well as reporting internally.

To submit a report within your organisation follow these useful steps:

If you suspect you have been contacted by a malicious profile online, the first thing you should do is report it to **your organisation** through the proper channels. Contact your **relevant security officer or line manager** with the following details:

- URL of the profile
- A screen shot of the message/request they sent
- A brief explanation of why you think the approach is suspicious
- Any other relevant details
- Disengage from the profile; don't interact any further

It's also important to report malicious activity to the relevant platform you are using. **When instructed by your security or line manager**, report malicious activity to the relevant social or professional networking platform. Each of these offers more detailed, platform-specific advice on their websites including reporting on fake or malicious profiles. For more information visit the help or report section on the website of the relevant platform you are using.

Remove

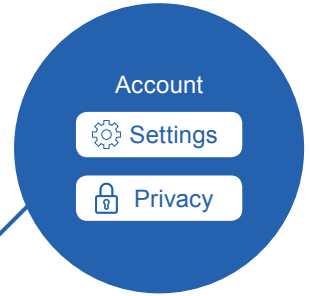
them from your network

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

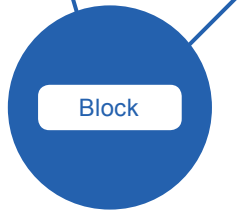
Encourage your trusted friends and colleagues to also remove these profiles if they have connected too.

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.



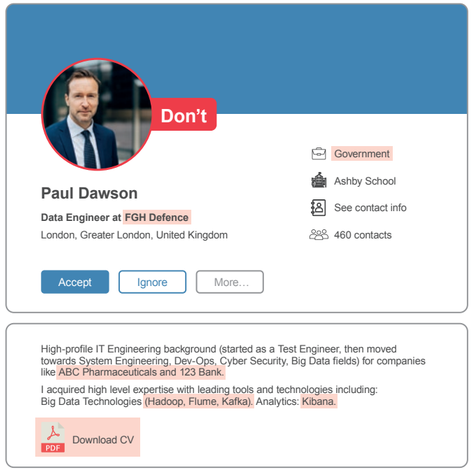
Many networking sites allow you to easily remove contacts just by accessing your directory and clicking on the relevant remove/block option for the malicious profile. You often do not need to click on the profile itself to do this.

Final tips

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

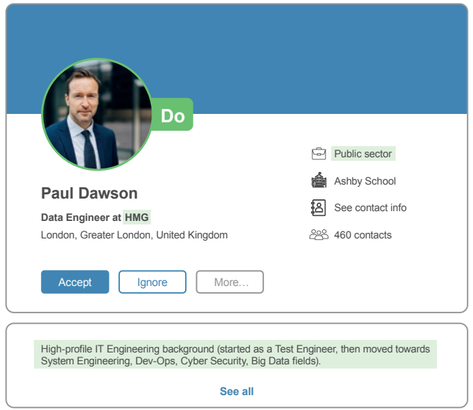
But there are some tips that can help you avoid being targeted in the first place.

Social and professional networking sites are there 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 this form of 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
- Make all your profile information publicly available



Do

- If necessary, include details of your security clearance in direct correspondence with genuine contacts
- If it's necessary to share sensitive details, such as a complete CV, or details of specific projects, do so one-to-one over trusted networks or in person with verified contacts
- Check your organisations 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).
- Users should take the time to find out and understand the profile settings available. The more personalised these settings are, the more control users have over their information.

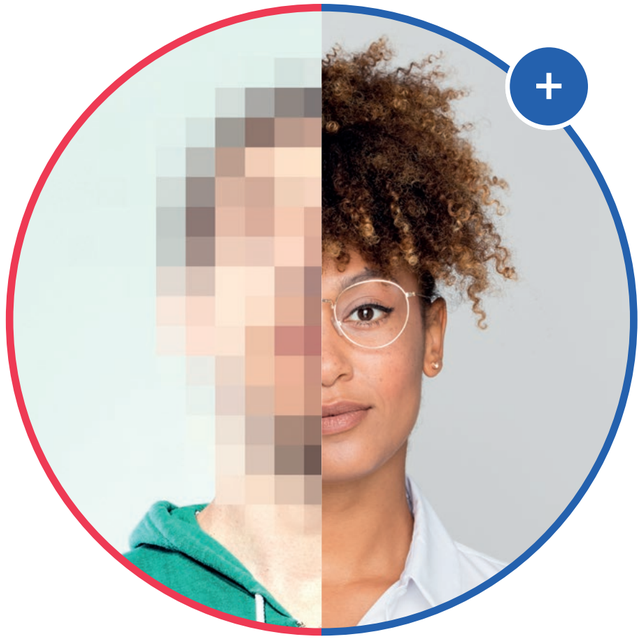
How should you network online safely?

Dealing with two audiences: the dual lens.

There are two audiences potentially viewing your profile – genuine professional contacts who support your credibility and raise your profile, and those who are out to exploit you and your organisation.

When managing your profile, you want to 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 what is the lowest level of detail that you need to provide in order for your profile to promote you properly to friendly audiences. What is the relevant information to potential talent hunters or recruiters? Does your profile give away 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:

R ecognise
the profile?

R ealise
the potential threat

R eport
to your Security Manager

R emove
them from your network

Crown copyright