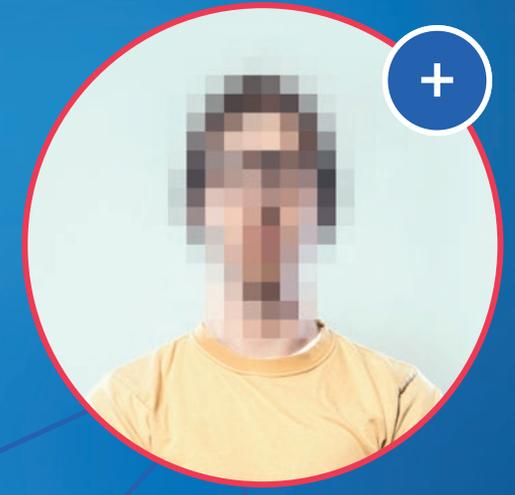




Think before you link

Staff briefing pack



The threat



What? Hostile actors using online platforms to approach individuals



Why? Recruitment of UK and Western nationals to act as unwitting agents and provide them with sensitive intelligence

Who? Those who:

- Identify as an employee or member of HMG or Civil Service
- 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)
- Mention that they have security clearances, especially Security Cleared (SC) or Developed Vetting (DV)



Don't

Paul Dawson

Data Engineer at **FGH Defence**

London, Greater London, United Kingdom

Accept

Ignore

More...

CPNI

Centre for the Protection
of National Infrastructure

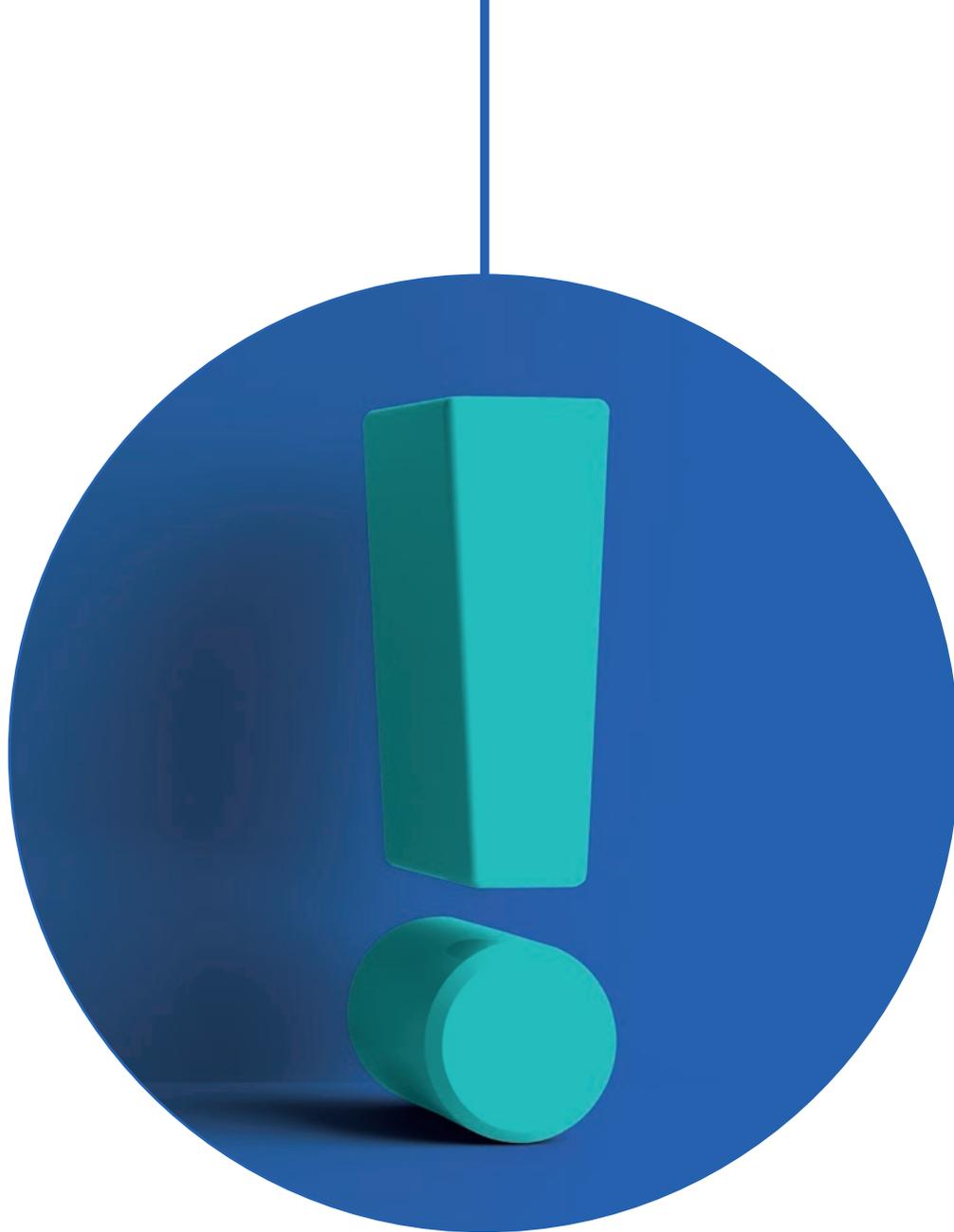


How?

- Initial engagement online presenting a 'unique' business offer
- Asks for further information about the individual and may request a CV
- Attempts to move away from the initial website to other platforms
- Set up phone calls or face to face discussions
- May be invited to another country to meet a representative

CPNI

Centre for the Protection
of National Infrastructure



Why is this relevant to you?

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

- Potential consequences of engaging with malicious profiles can be serious (e.g. loss of security clearance)
- Our staff are vulnerable to attack
- Campaign resources designed to help you protect yourselves and your organisation from being manipulated

Know the signs!

CPNI

Centre for the Protection
of National Infrastructure

Countering the Threat

Recognise

the profile?

Realise

the potential threat

Report

to your Security Manager

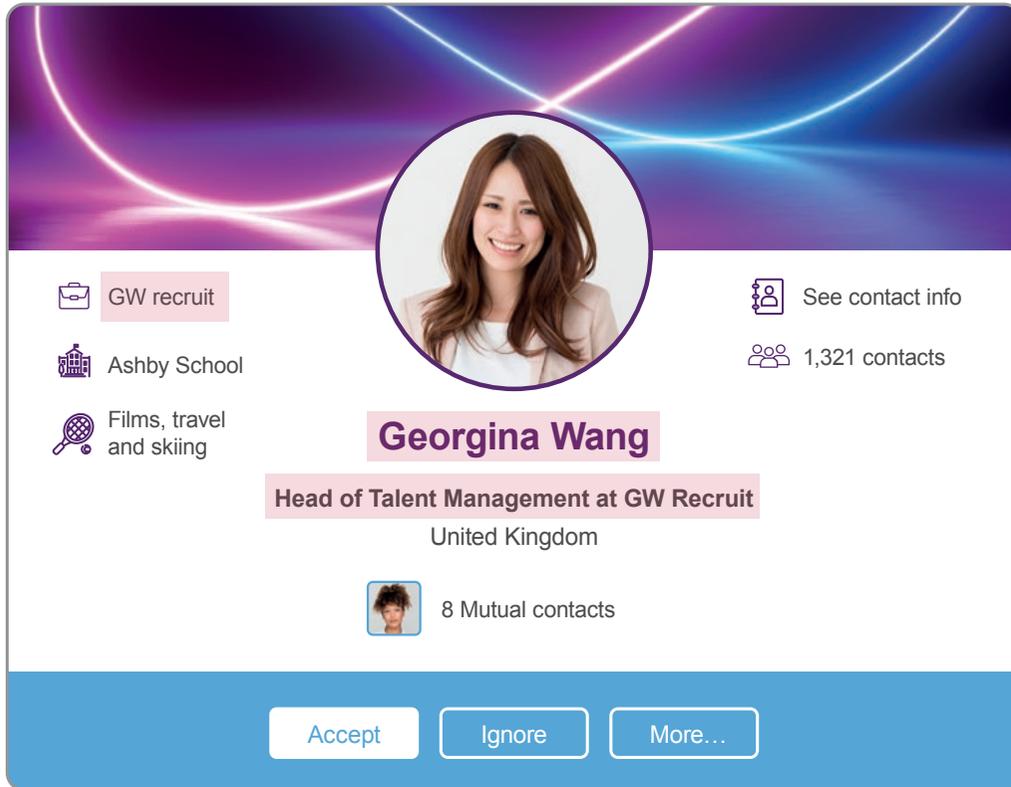
Remove

them from your network

CPNI

Centre for the Protection
of National Infrastructure

Recognise the profile?



A screenshot of a LinkedIn profile for Georgina Wang. The profile features a circular profile picture of a woman with long brown hair. To the left of the picture are three icons: a briefcase for 'GW recruit', a school building for 'Ashby School', and a tennis racket for 'Films, travel and skiing'. To the right are icons for 'See contact info' and '1,321 contacts'. Below the picture, the name 'Georgina Wang' is displayed in a pink box, followed by her title 'Head of Talent Management at GW Recruit' and location 'United Kingdom'. At the bottom left, there is a small profile picture of another person and the text '8 Mutual contacts'. At the bottom of the profile card are three buttons: 'Accept', 'Ignore', and 'More...'. The background of the profile card has a purple and blue abstract design.

GW recruit

Ashby School

Films, travel and skiing

See contact info

1,321 contacts

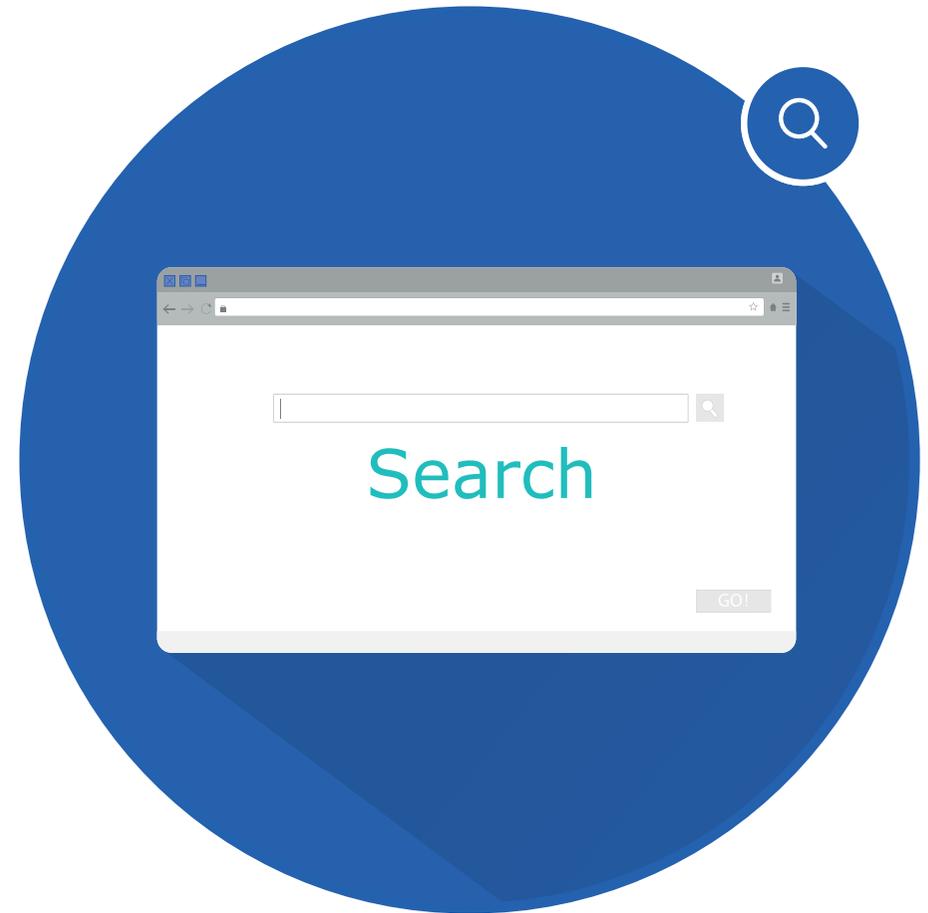
Georgina Wang

Head of Talent Management at GW Recruit

United Kingdom

8 Mutual contacts

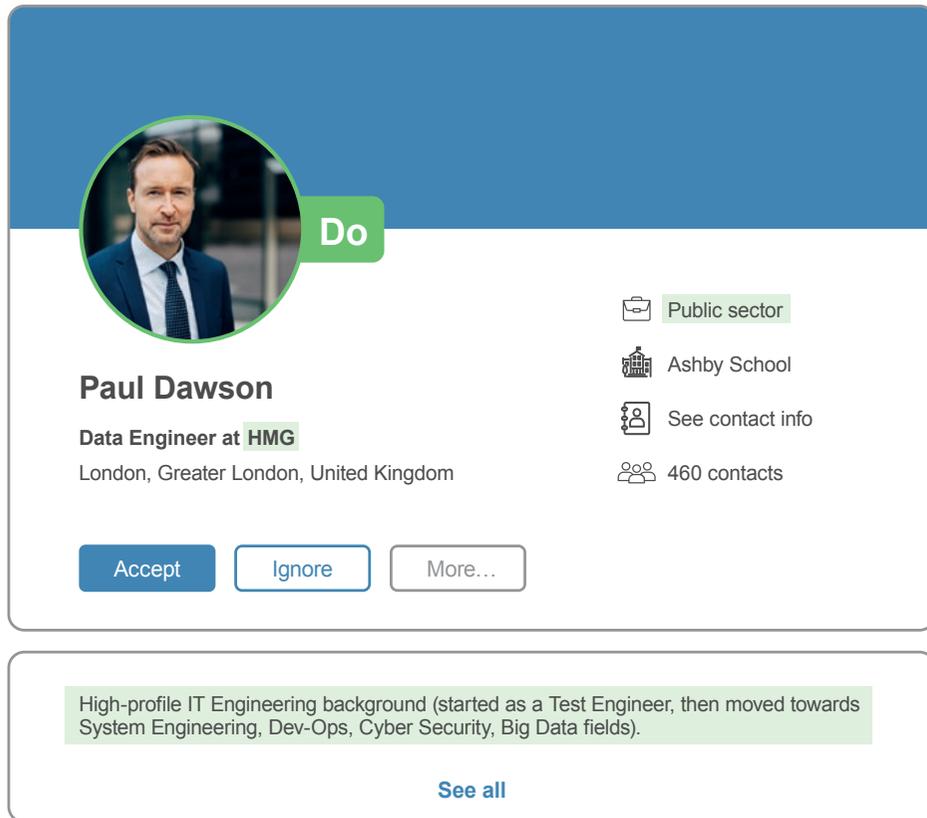
Accept Ignore More...



CPNI

Centre for the Protection
of National Infrastructure

Realise the Threat



A LinkedIn profile card for Paul Dawson. The card features a circular profile picture of a man in a suit and tie. To the right of the picture is a green badge with the word "Do". Below the picture, the name "Paul Dawson" is displayed in bold, followed by "Data Engineer at HMG" and "London, Greater London, United Kingdom". To the right of the name are four icons with corresponding text: a briefcase icon for "Public sector", a school icon for "Ashby School", a person icon for "See contact info", and a group of people icon for "460 contacts". At the bottom of the card are three buttons: "Accept", "Ignore", and "More...". Below the card is a green highlighted box containing the text: "High-profile IT Engineering background (started as a Test Engineer, then moved towards System Engineering, Dev-Ops, Cyber Security, Big Data fields)." and a "See all" link.

Do

Paul Dawson
Data Engineer at HMG
London, Greater London, United Kingdom

Public sector
Ashby School
See contact info
460 contacts

Accept Ignore More...

High-profile IT Engineering background (started as a Test Engineer, then moved towards System Engineering, Dev-Ops, Cyber Security, Big Data fields).

[See all](#)

Genuine recruitment approaches

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

- Progress at the candidate's pace, not the recruiters
- Validate you as a candidate
- Attempt to make life easier for the candidate
- Manage expectations of the candidate

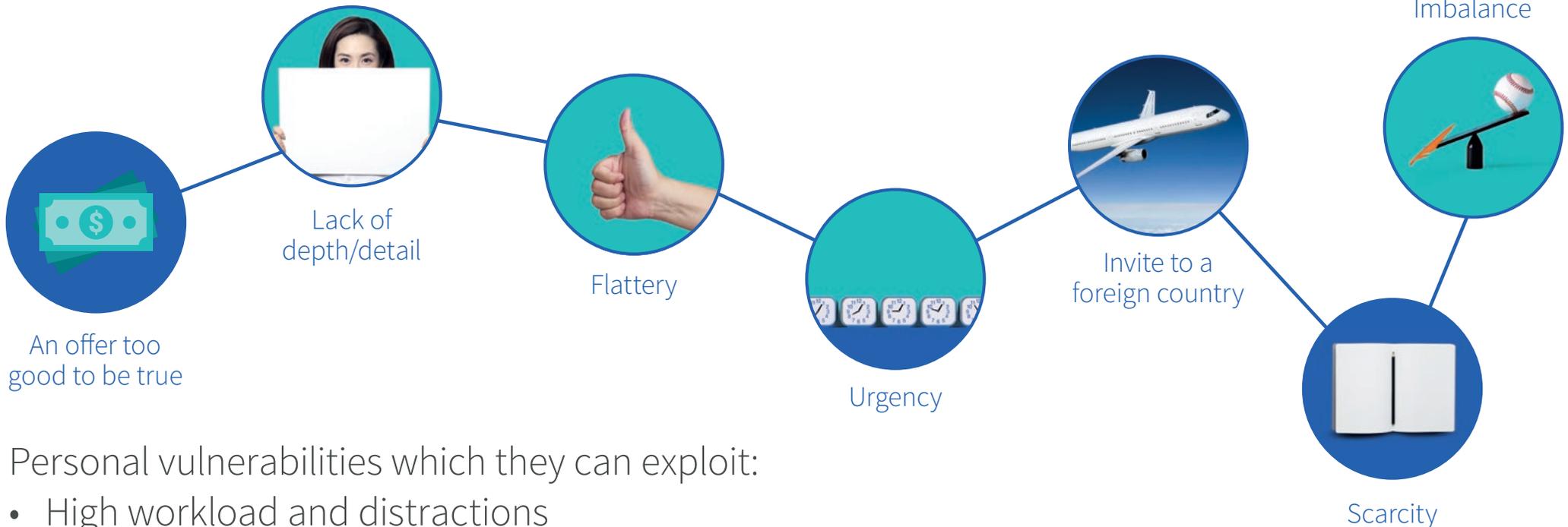
CPNI

Centre for the Protection
of National Infrastructure

Realise the Threat

Illegitimate recruitment approaches

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



Personal vulnerabilities which they can exploit:

- High workload and distractions
- Recent job or life changes (e.g. unemployment, retirement)
- Appealing to your identity as a professional and values such as being valued, respected, rewarded etc.

CPNI

Centre for the Protection
of National Infrastructure

Report to your security manager

- Do not engage
- Report to the Security Manager or line manager
- Profile URL
- 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 will be treated with discretion and taken seriously

CPNI

Centre for the Protection
of National Infrastructure

Remove them from your network

GW recruit

Ashby School

Films, travel and skiing

See contact info

1,321 contacts

Georgina Wang

Head of Talent Management at GW Recruit

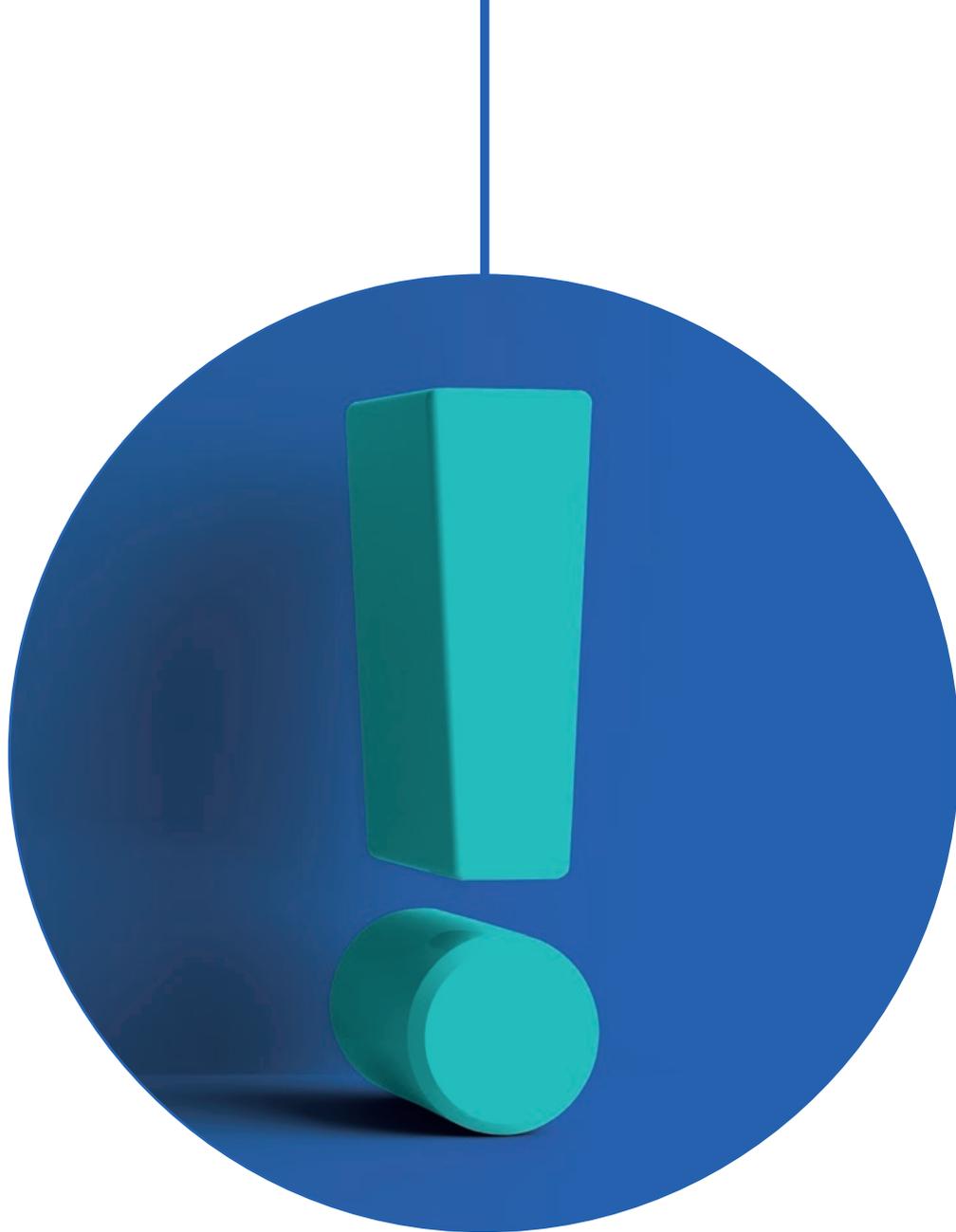
United Kingdom

8 Mutual contacts

Accept Ignore More...

CPNI

Centre for the Protection
of National Infrastructure



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
- Think 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 control who can view your profile
- Only share CVs or details of specific projects with trusted and verified contacts

Any questions?

CPNI

Centre for the Protection
of National Infrastructure