Think before you link

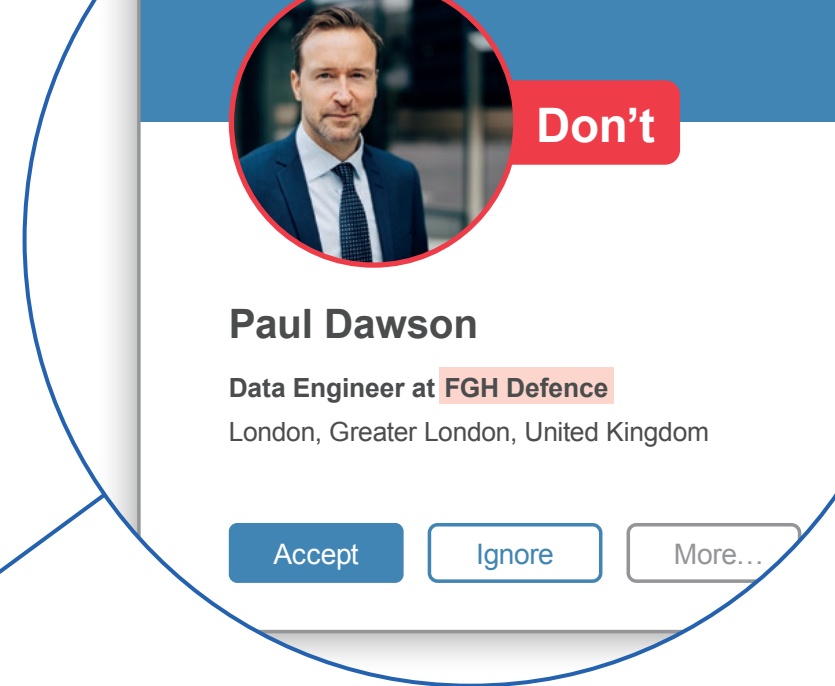**Staff briefing pack**
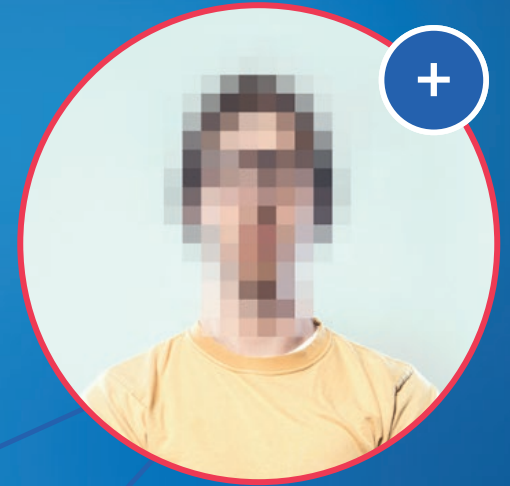
Branding

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

Don't

Paul Dawson

Data Engineer at FGH Defence

London, Greater London, United Kingdom

Accept | Ignore | More...

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)

CPNI
Centre for the Protection
of National Infrastructure
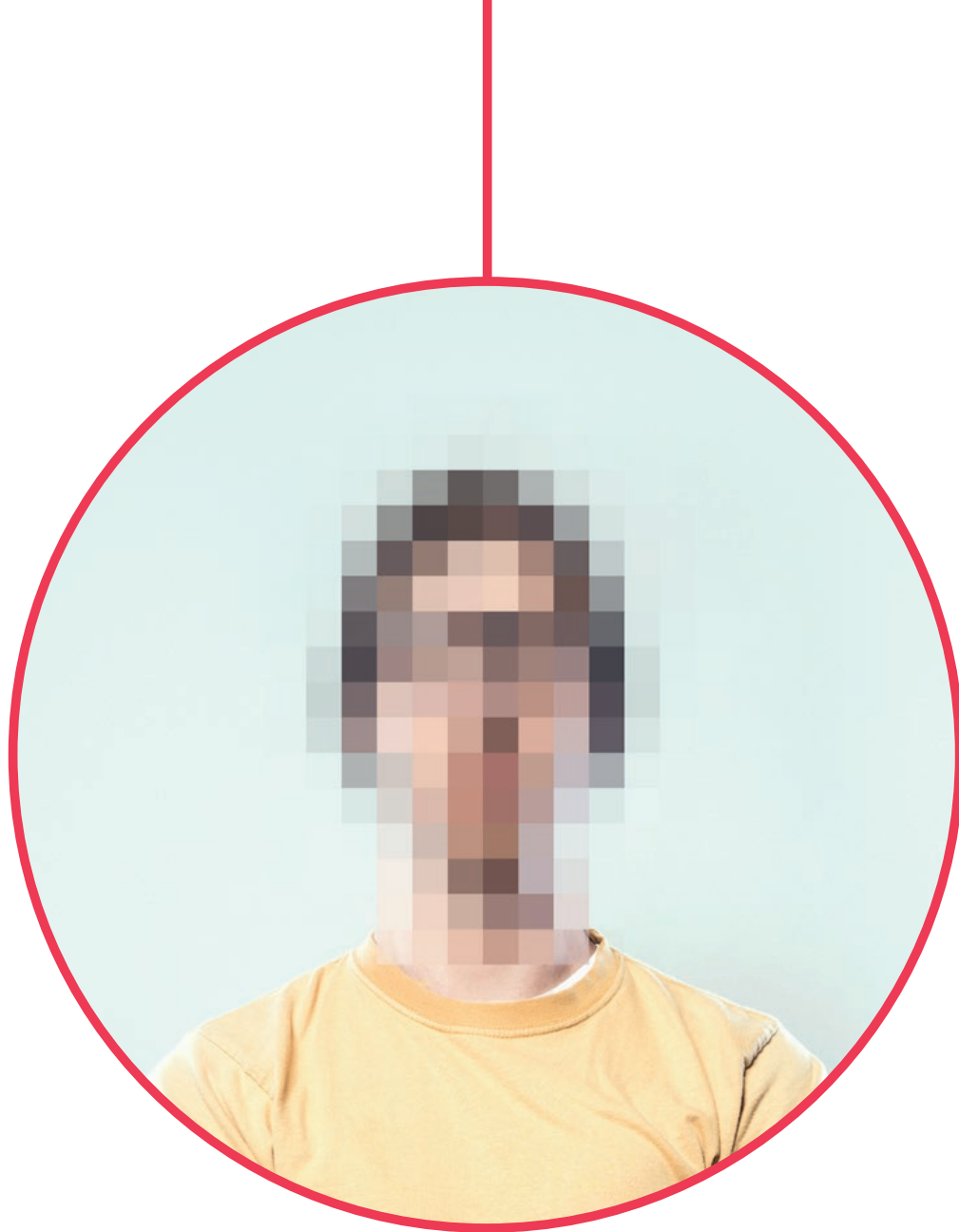
How?

- 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
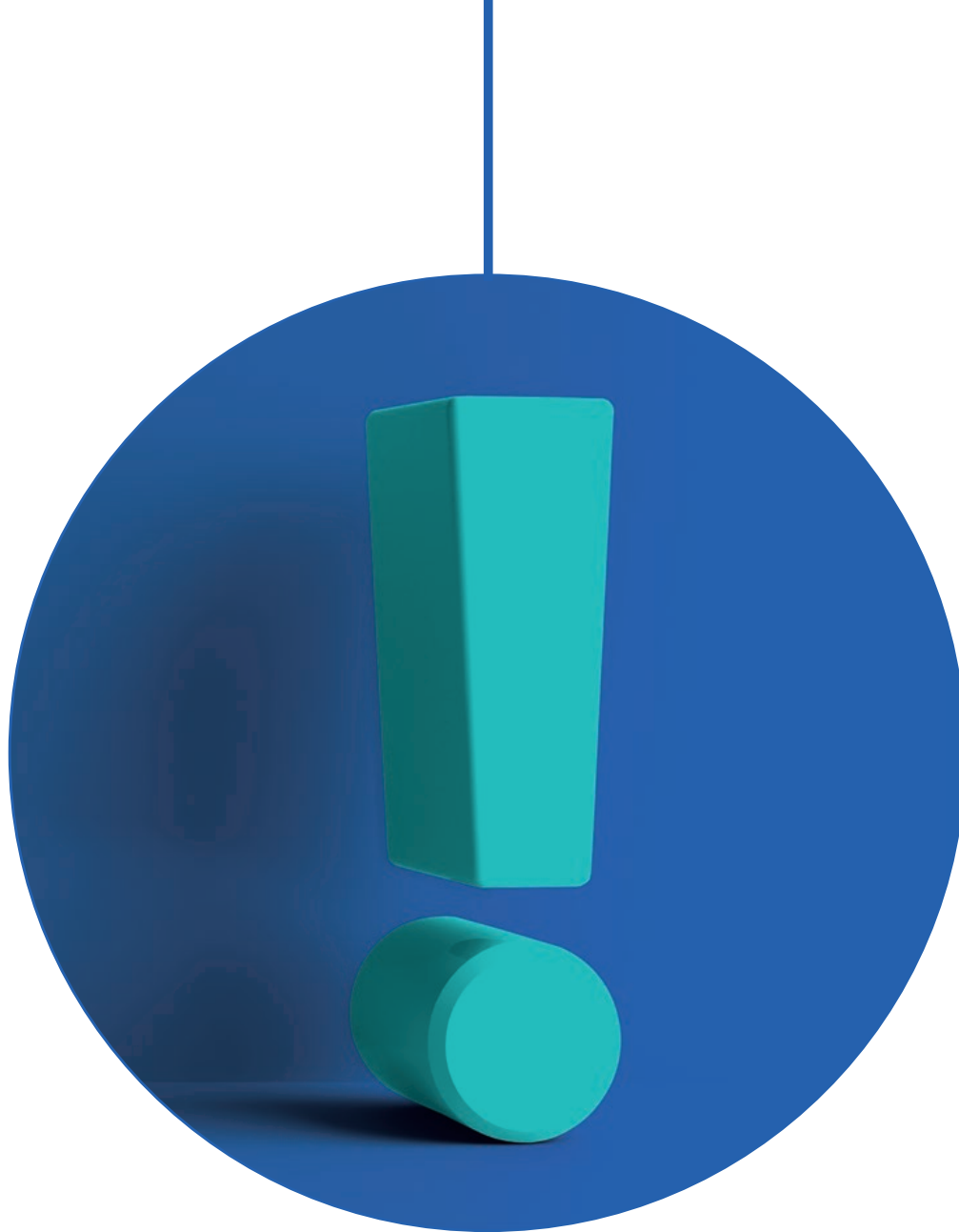
Why is this relevent to you?

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
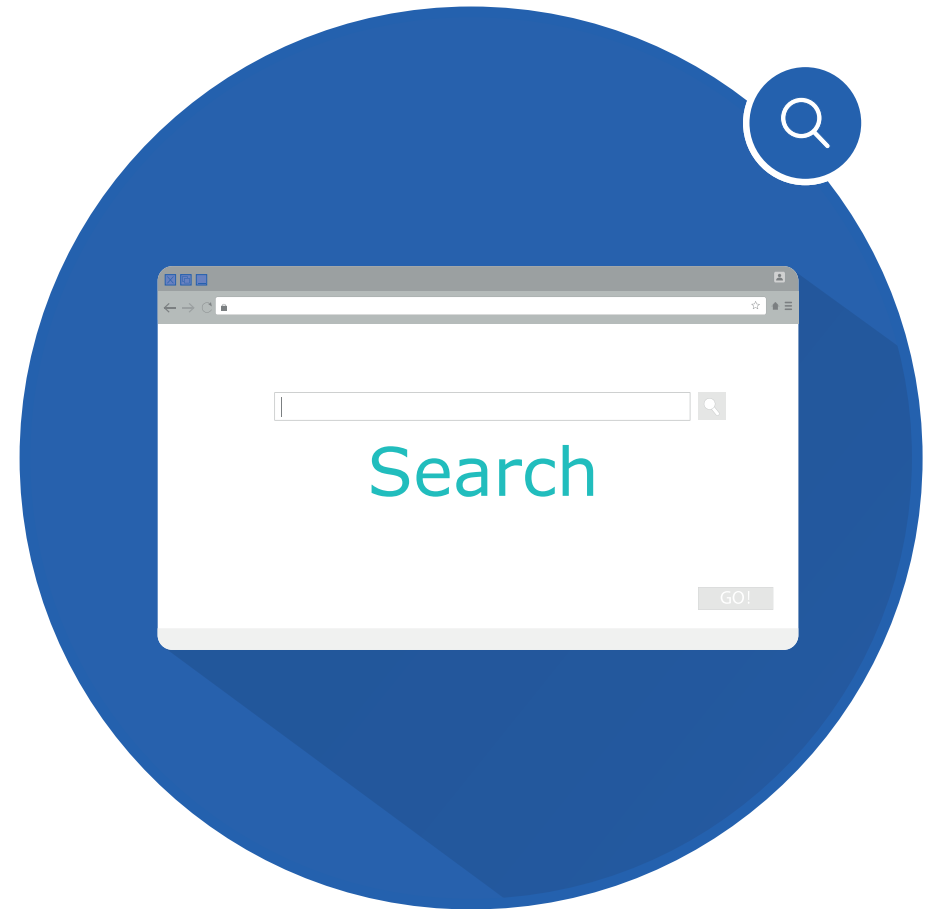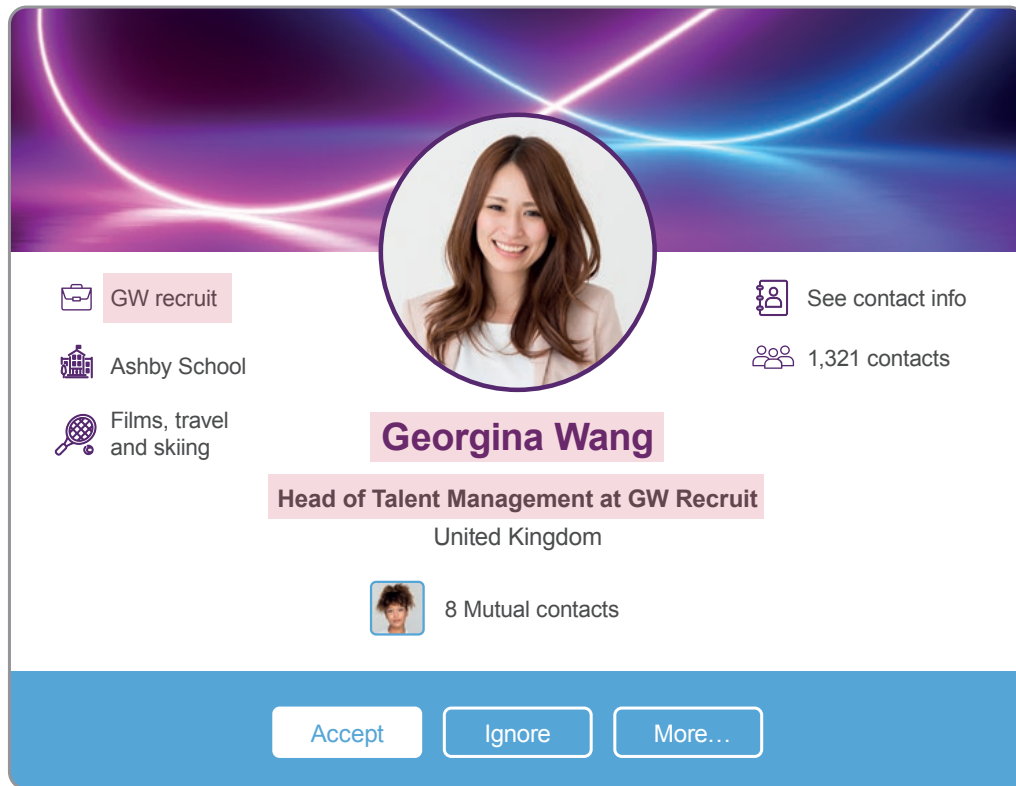
Report
to your Security Manager

Remove
them from your network

CPNI
Centre for the Protection
of National Infrastructure

Recognise the profile?

GW recruit

Ashby School

Films, travel and skiing

Georgina Wang

Head of Talent Management at GW Recruit

United Kingdom

See contact info

1,321 contacts

8 Mutual contacts

Accept | Ignore | More…

Search

GO!

Realise the Threat

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
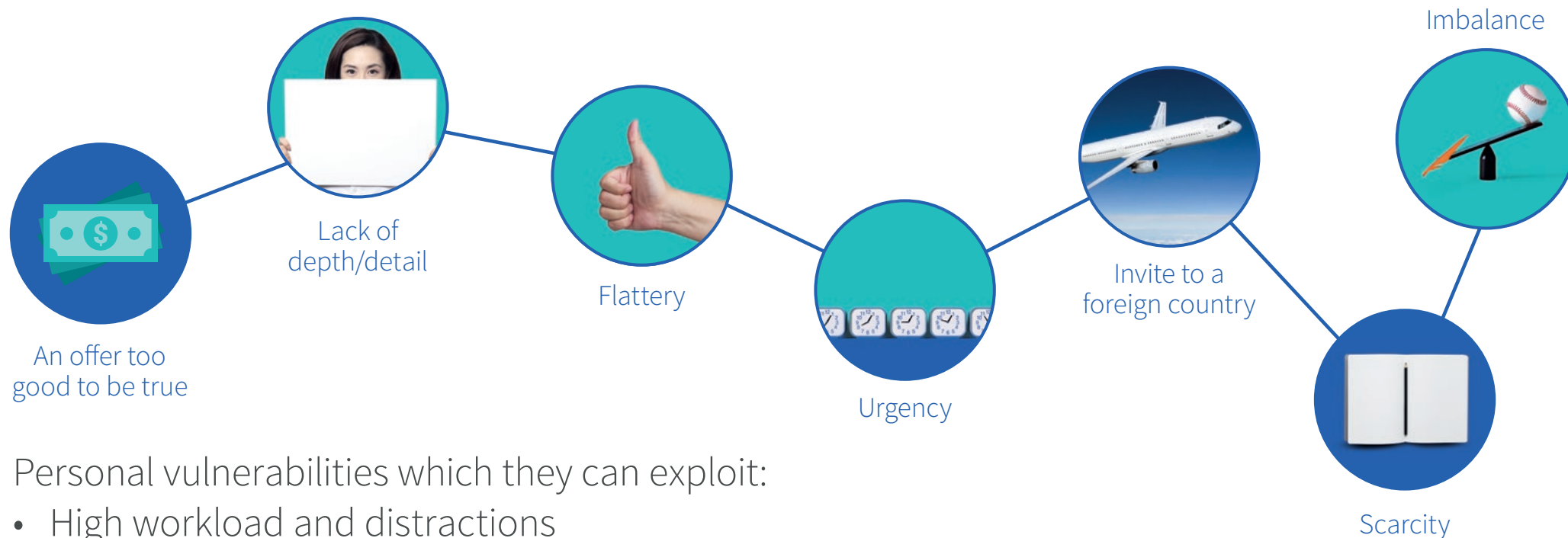
- Progress at the candidate's pace, not the recruiters

- Validate you as a candidate

- Attempt to make life easier for the candidate

- Manage expectations of the candidate

Realise the Threat

Illegitimate recruitment approaches

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

Imbalance

Lack of
depth/detail

Flattery

An offer too
good to be true

Urgency

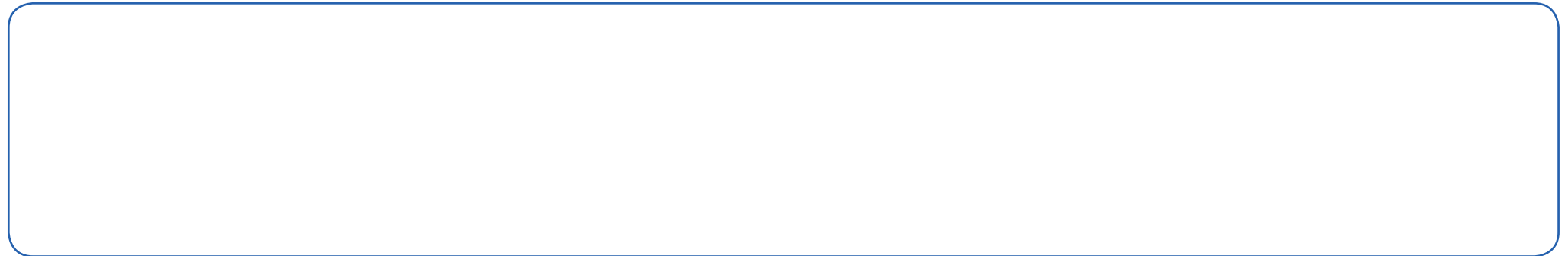Invite to a
foreign country

Scarcity

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.
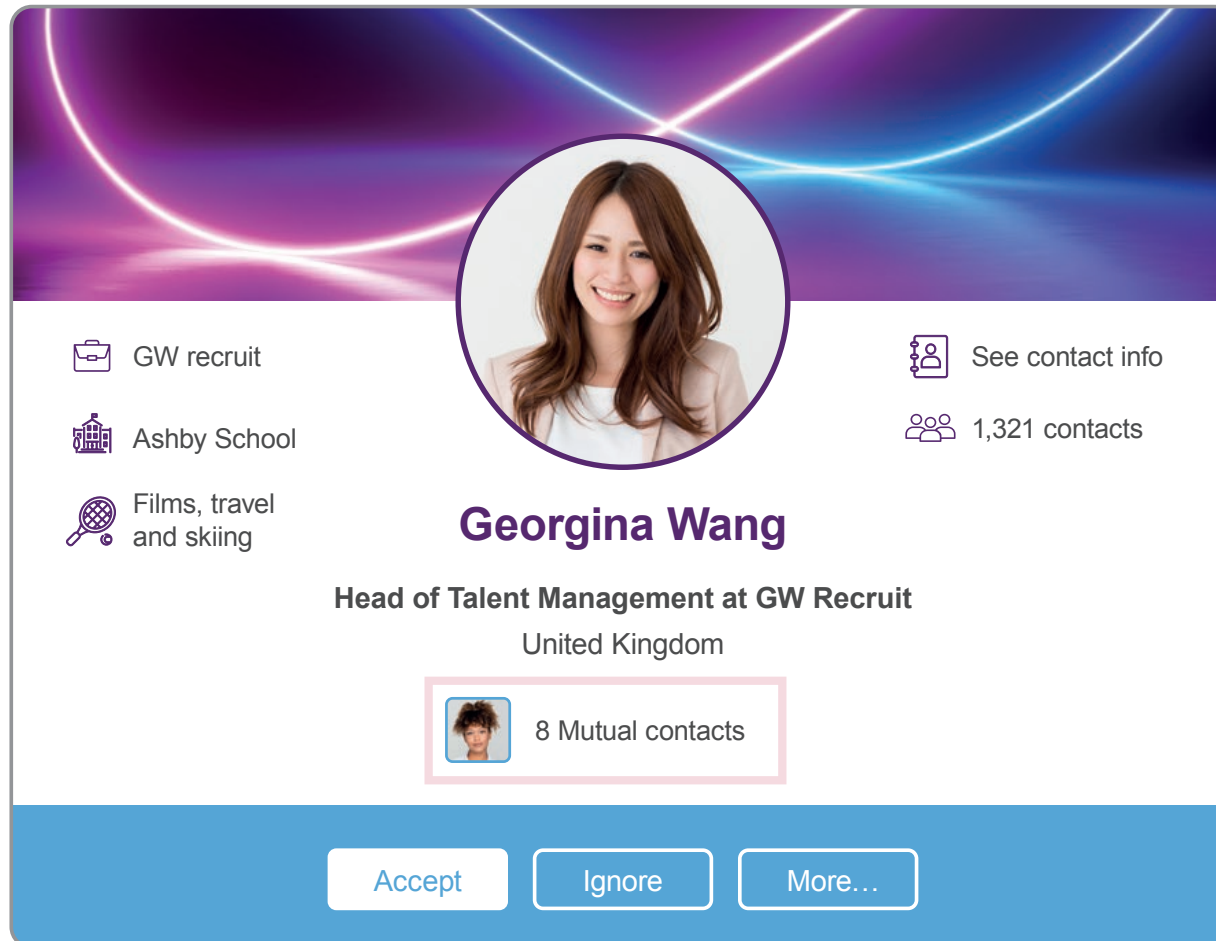
CPNI
Centre for the Protection
of National Infrastructure

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…

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