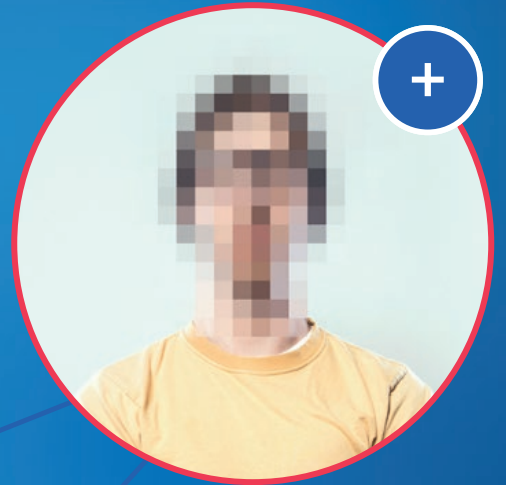




Think before you link

Senior briefing pack

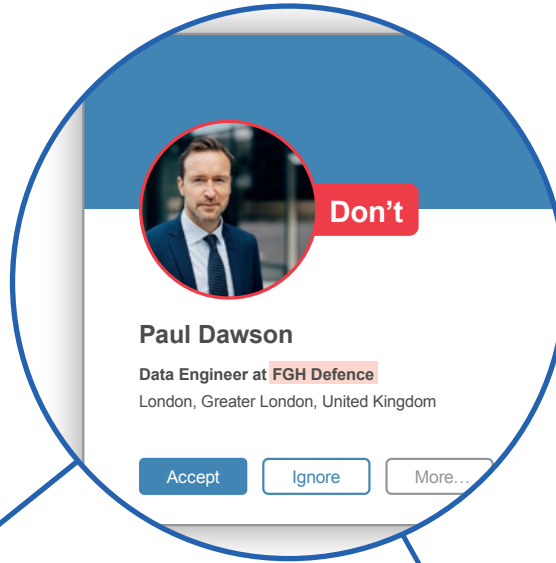


1. What is the threat?
2. Key advice
3. Benefits of the campaign
4. Campaign materials
5. Time and resourcing

The Threat

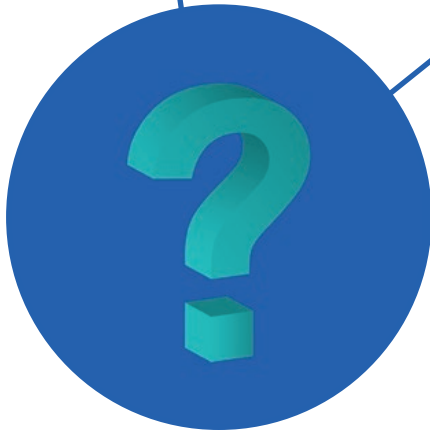


What? Hostile actors using online platforms to approach individuals.



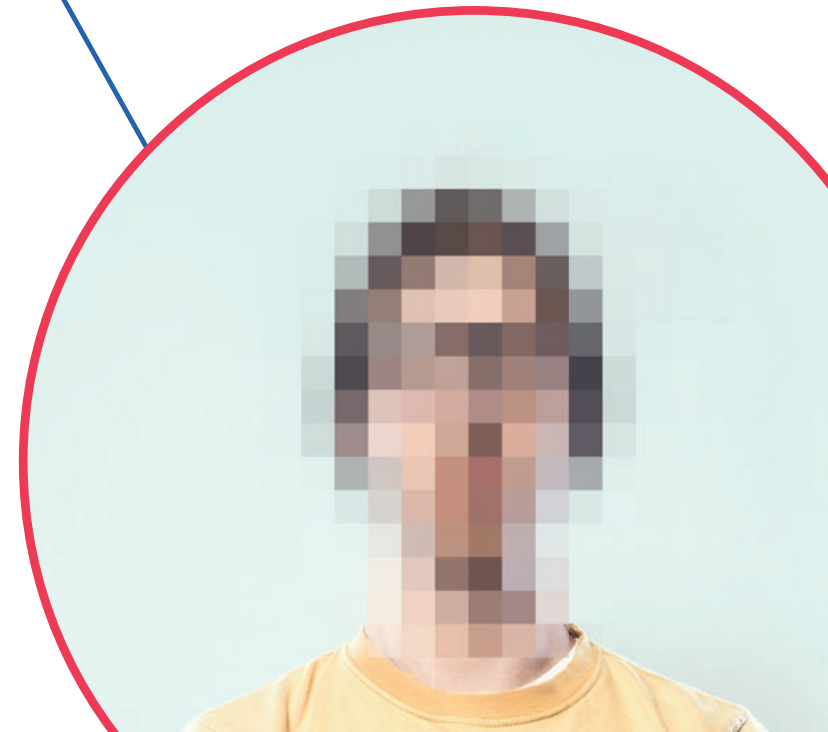
Who? Those who:

- 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)



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

How? Approaching individuals online offering 'unique' business opportunities



CPNI

Centre for the Protection of National Infrastructure

Advice given– the 4 R's

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

Also how to not make yourself a target online in the first place.



Why is this relevant to you?

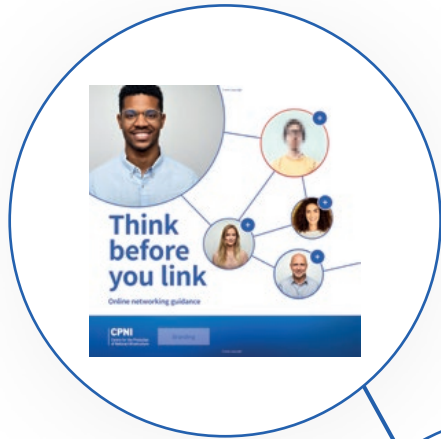
- It raises awareness of the threat amongst staff
- Motivates users to be vigilant and take appropriate action
- Encourages users to take action to prevent making themselves a target online
- The consequences of engaging with these profiles can be extremely damaging
- It makes it harder for malicious profiles to use social and professional networks to target individuals.

CPNI

Centre for the Protection
of National Infrastructure

Campaign materials

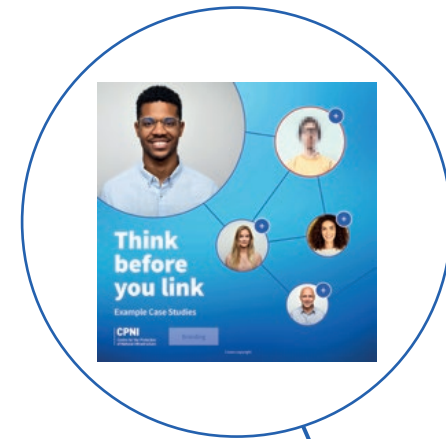
Guidance for staff



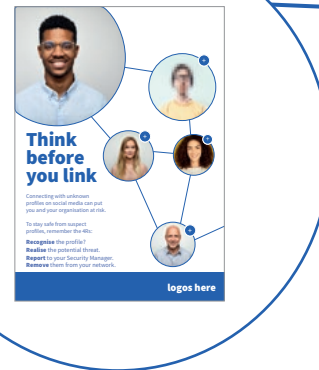
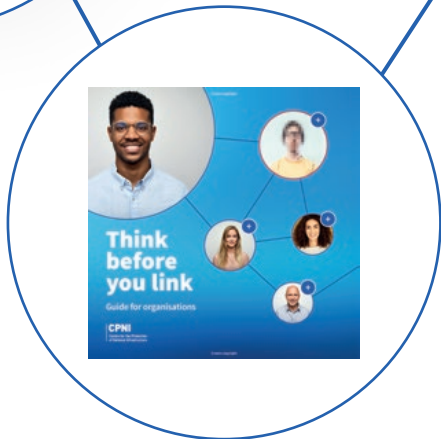
Staff slide decks



Case studies



Guidance for organisations



Poster sets



Wallet cards

CPNI

Centre for the Protection
of National Infrastructure

Time and resources

Pre-campaign 4-6 weeks		Live campaign 12 weeks		Post-campaign 4 weeks post-campaign	
Activities	Resources	Activities	Resources	Activities	Resources
<ul style="list-style-type: none"> Stakeholder engagement 	<ul style="list-style-type: none"> Senior Briefing packs 	<ul style="list-style-type: none"> Briefings to key staff 	<ul style="list-style-type: none"> Staff briefing packs 	<ul style="list-style-type: none"> Evaluate reporting statistics 	<ul style="list-style-type: none"> CPNI Embedding Security Behaviours Using the 5Es
<ul style="list-style-type: none"> Gain senior Buy-in 	<ul style="list-style-type: none"> Organisation guide 	<ul style="list-style-type: none"> Communications from senior figures/relevant experts 	<ul style="list-style-type: none"> Posters 	<ul style="list-style-type: none"> Post-campaign surveys or focus groups 	<ul style="list-style-type: none"> CPNI Guidance: Evaluation Guide for Internal Security Behaviour Campaigns
<ul style="list-style-type: none"> Develop a communications plan 	<ul style="list-style-type: none"> CPNI Embedding Security Behaviours Using the 5Es 	<ul style="list-style-type: none"> Launch poster materials 	<ul style="list-style-type: none"> Staff guide 	<ul style="list-style-type: none"> Monitor other feedback channels 	<ul style="list-style-type: none"> Organisation Guide
<ul style="list-style-type: none"> Prepare or adapt materials 		<ul style="list-style-type: none"> Embed briefings and materials into existing delivery mechanisms (e.g. new joiners) 	<ul style="list-style-type: none"> Flyer 	<ul style="list-style-type: none"> Maintain upkeep of campaign materials for ongoing security briefings (e.g. induction, leavers). 	
<ul style="list-style-type: none"> Review reporting mechanisms 			<ul style="list-style-type: none"> Case studies 		
<ul style="list-style-type: none"> Baseline evaluation metrics 			<ul style="list-style-type: none"> Supporting materials 		

Posters with 4 R's



Think before you link

Connecting with unknown profiles on social media can put you and your organisation at risk.

To stay safe from suspect profiles, remember the 4Rs:

- Recognise** the profile?
- Realise** the potential threat.
- Report** to your Security Manager.
- Remove** them from your network.

logos here



Connection or con?

Your new connections aren't always who they say, and this can put you and your organisation at risk.

To stay safe from suspect profiles, remember the 4Rs:

- Recognise** the profile?
- Realise** the potential threat.
- Report** to your Security Manager.
- Remove** them from your network.

logos here

CPNI

Centre for the Protection
of National Infrastructure

Any questions?

CPNI

Centre for the Protection
of National Infrastructure