Introduction

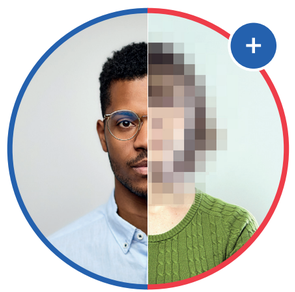
This document is designed to help staff understand the types of approaches you might encounter from malicious profiles online by presenting true-to-life examples. CPNI has conducted research to establish the common traits amongst these malicious approaches, to help enable people to more readily identify when they are the target of a potential malicious approach online.

This research has informed the development of a detailed case study based on the experiences of real cases where individuals were targeted and had begun to engage with the malicious profiles, sometimes with serious implications. The case studies within are not direct accounts of specific individuals' experiences, but a reflection of the types of experience that might be typical for the victim of a malicious approach online.

If you work in an organisation **with access to sensitive data or assets** you are **vulnerable** to this type of malicious approach and should take steps to educate yourself about the threat and **reduce your risk** of being targeted.

Reading these case studies may help you to identify when you or your colleagues are in a situation that could pose you, them, or your organisation harm.

No one is immune to being socially manipulated into wrongdoing through these approaches – malicious profiles are deliberately trying to exploit vulnerabilities that are inherent in all people. It could happen to you. Knowing the warning signs and managing your digital footprint are the best defences to protect against malicious profiles.

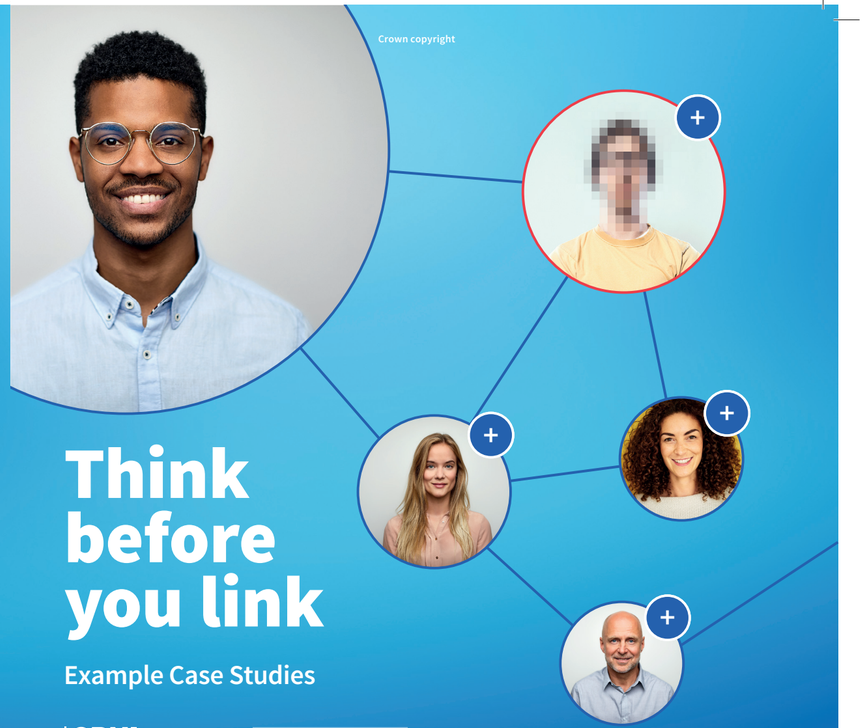


Recognise
the profile?

Realise
the potential threat

Report
to your Security Manager

Remove
them from your network



Think before you link

Example Case Studies

CPNI
Centre for the Protection of National Infrastructure

Branding

Case Study 1: Matthew

Background:

Matthew was a DV-cleared UK civil servant working overseas. His professional networking profile included his e-mail address and his employment history. This employment history mentioned his previous area of expertise in government which, **by association, indicated that Matthew held sensitive security clearance**.

Digital Footprint

Think carefully about the information you display publicly online as this can make you a target for malicious profiles. Refer to the guide for how best to shape your profile!

The approach:

Matthew was approached on the networking site by an individual, allegedly called Helen, who claimed to work for a think tank with a business proposition. Matthew had not heard of the think tank or the recruiter before which felt a little unusual to him. However, after checking their shared contacts he found that they had a **friend in common and therefore assumed the profile must be genuine**. Matthew explained away his doubts and decided to accept the connection.

Common Contacts

Don't assume that people in your network have checked out their contacts. Just because you have a mutual contact does not mean the profile is always genuine.

The recruiter quickly contacted Matthew directly, **flattering his skillset** and outlining an attractive consultancy opportunity.

Flattery

Malicious profiles use flattery to establish contacts and keep targets engaged. Be sceptical until you get some signs that the profile is genuine.

The offer was **vague and did not include specific details** of the role. Matthew was not entirely clear what this consultancy opportunity would entail but presumed that the think tank would not disclose this information until they had interviewed him. When he asked for specifics, the recruiter explained the need to retain client confidentiality and Matthew felt satisfied by this. Having worked in the Civil Service, Matthew thought this demonstrated a level of discretion and professionalism.

Lack of Detail

Malicious profiles use vague language to describe their business opportunities. If no specifics are forthcoming you should be very suspicious.

Engagement:

After exchanging a number of messages over a period of approximately one month, the recruiter suggested moving to personal emails. Contact became more frequent, which seemed a little persistent but **Matthew felt flattered by their interest in him**. Matthew was more focused on the offer as it **seemed like the perfect job opportunity**.

The so-called recruiter and Matthew discussed recent international events, with the recruiter seeking Matthew's opinion based on his skills and expertise. The recruiter had always seemed very informal and friendly in her messages.

Matthew wanted to appear respectful and polite in return so when the recruiter suggested a face-to-face meeting, he accepted. The two subsequently communicated by e-mail, instant message, and telephone call, as well as meeting on several occasions.

Too Good to Be True

If you're approached with an opportunity that seems too good to be true, it probably is!

It was only when Matthew's brother questioned his interaction with the recruiter that Matthew became suspicious. His brother suggested the offer may be **'too good to be true'**. At this point Matthew broke contact with the recruiter. Despite these suspicions, Matthew did not mention the approach in his vetting renewal interview.

Reporting

If you've had a suspicious interaction online your organisation's security team may want to know about this. Reporting this activity helps protect yourself, your colleagues and your organisation.

Case Study 2: Emma

DV-cleared Ex Civil Servant

- Approached online over a professional networking site
- Travelled to a foreign country for meetings
- Over a six-month period Emma was recruited and provided with basic covert communications system to provide information to contacts
- Emma was asked to provide sensitive information in relation to HMG

Case Study 3: Jason

SC-cleared Engineer at UK Defence Contractor

- Approached online over a professional networking site
- Travelled to a foreign country for meetings with contacts established online
- Was asked for detailed technical information on military aircraft
- Arranged to travel to a foreign country for a third time before being disrupted by the Security Service