Think before you link

Case Studies based on real examples of malicious online profiles

PSR | Protective Security Requirements

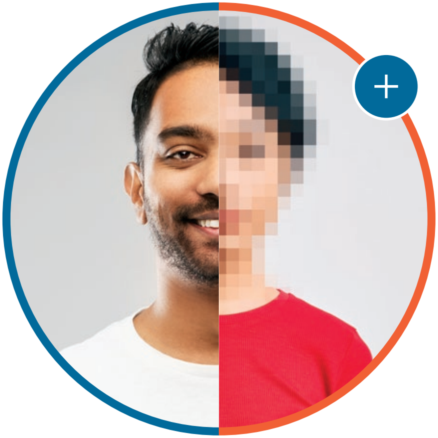
About these case studies

Read these case studies to help you understand the types of malicious profiles you might encounter online, so you can protect yourself and your organisation from harm.

No one is immune from being manipulated into wrongdoing through online approaches from people with malicious intentions. Individuals and groups, such as foreign state actors and criminals, try 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 against this threat.

These case studies are based on research conducted in the United Kingdom that established the common traits among these malicious online approaches. To protect people's privacy, these case studies are not direct accounts. However, they reflect what people typically experience when they fall victim to a malicious online approach.

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



Case Study 1:
Matthew gets a promising job offer

Matthew was a New Zealand public servant working overseas. He used to hold a national security clearance.

What was on his networking profile?

Matthew's professional networking profile included his:

- email address
- employment history.

His employment history mentioned his previous area of expertise, which made it obvious that Matthew had access to sensitive government information.

Be careful with your digital footprint

Think carefully about the information you display publicly online, as it can make you a target.

Do not disclose that you have:

- access to classified or commercially-sensitive information, technology, or research
- a national security clearance.

How was he approached?

Matthew was approached on a networking site by someone called Helen. She claimed to work for a think tank and have a business proposition for him.

Matthew hadn't heard of the think tank or the recruiter before, which felt a little unusual to him. However, after checking their shared contacts he found they had a friend in common, so he assumed the profile was genuine. Matthew felt he had overcome his doubts and decided to accept the connection.

Common contacts don't mean an online profile is genuine

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 genuine.

What happened next?

The recruiter quickly contacted Matthew and was flattering about his skillset. They then outlined an attractive consultancy opportunity.

The offer was vague and didn't include specific details of the role. Matthew wasn't entirely clear what this consultancy opportunity would entail, but he assumed the think tank wouldn't disclose this information until they'd interviewed him.

When Matthew asked for specifics, the recruiter explained the need to retain client confidentiality and Matthew felt satisfied by this answer. Having worked in the public service, Matthew thought she was demonstrating discretion and professionalism.

Beware of flattery

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

Be suspicious of a lack of detail

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

How was he lured into more contact?

After exchanging a number of messages over a few weeks, the recruiter suggested moving to personal emails. Contact became more frequent, which seemed a little persistent but Matthew felt flattered by the think tank's interest in him. He was focused on the job offer as it seemed like a perfect 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 email, instant message, and phone calls, as well as meeting in person on several occasions.

Beware of requests for your personal contact details or to meet in person

Requesting your personal contact details is a known tactic. Don't hand them over!

Why did he eventually stop the contact?

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 his suspicions, Matthew didn't immediately report the approach to his manager or through any of the channels he was expected to use as a national security clearance holder.

Be wary of offers that seem too good to be true

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

Report all suspicious approaches and contact

If you've had a suspicious interaction online, your organisation's security team need to know about it. Report what happened so they can protect you, your colleagues, and your organisation.

Brief examples of other malicious approaches

Case Study 2: Emma

Former public servant with a national security clearance

- 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 a basic covert communications system to provide information to contacts
- Emma was asked to provide sensitive information potentially damaging to the New Zealand government.

Case Study 3: Jason

Contracted computer engineer working on a sensitive system with a national security clearance

- 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 computer systems
- Arranged to travel to a foreign country for a third time before being disrupted.

Recognise

a suspicious profile

Realise

the potential threat

Report

your concerns

Remove

them from your network

The information in this booklet is based on research carried out by the Centre for Protection of National Infrastructure (CPNI). CPNI is the government authority for protective security advice to the UK national infrastructure. www.cpni.gov.uk