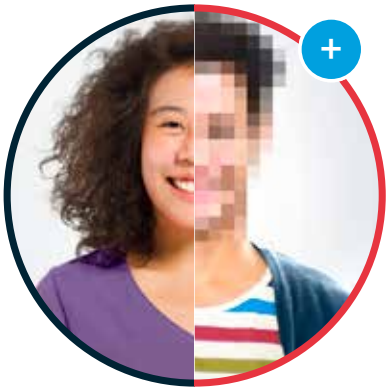
Australian Government

Australian Security Intelligence Organisation

ASIO

Think before you link

Case study



Introduction

This document aims to help you understand the types of malicious approaches you might encounter from individuals online. The example demonstrates the common features of these approaches and should allow you to more readily identify when you are the target of a potential malicious approach online. If you work in an organisation with access to sensitive data or assets, you are more likely to be targeted by this type of malicious approach and you should take steps to reduce your risk.

Consider what information about you is available online, and how this could contribute to you or your colleagues being misled or placed in a situation that could harm you, them, your organisation or your country. The following case study identifies some of the common warning signs of a potentially malicious approach.

No one is immune from being manipulated into wrongdoing through such approaches, and foreign intelligence services deliberately attempt to exploit vulnerabilities inherent in all people. These approaches are more common than you might think—it could happen to you. Knowing the warning signs and managing your digital footprint are the best defences to protect against malicious approaches.

Case study: Jack

Background

Jack is an Australian Government clearance holder. He established a profile on a professional networking site for employment opportunities. His profile information mentioned his areas of expertise in government. When considered with other information available online, it was clear that Jack would have access to classified and sensitive information. Although Jack was confident he limited who could see this information, it was still available to those who might pose as a recruitment company on the networking site.

The approach

Jack was contacted by a representative of a consulting company via the networking site. It was not a company that Jack had heard of before. However, on searching the company's profile, Jack observed the company was a common contact of many individuals who worked in the same industry as him, and that it maintained a social media presence relevant to his area of expertise. This gave Jack confidence that the approach was genuine, and he responded to the initial contact using the networking site's messaging platform.

The individual who sought contact with Jack then organised a virtual meeting with him, via a publicly available encrypted communications application. During this virtual meeting, the consulting company representatives noted that Jack had a unique and valuable range of skills and experience, making him a perfect candidate to undertake very lucrative consultancy work for their company.

Jack sought details to confirm the nature of the offer, and the contact information for the company. The company representatives noted the specific details of their offer were proprietary and would be better discussed in person. They asked Jack to contact them only via the same encrypted communications application or through direct communication with the representative, rather than through more general company communication methods.

Engagement

After this initial exchange, Jack was offered an all-expenses-paid trip to discuss the details of the role. They also stressed to Jack that the role would need him to travel semi-regularly for discussions about the more sensitive components of the role. The representatives noted they were very impressed with Jack's professional experience and didn't want to lose the opportunity to work with him.

Although initially suspicious, Jack didn't want to turn down a job opportunity that aligned so well with his skillset. However, as the communication with the company continued, Jack began to consider that the company and job on offer might not be genuine. He considered the very real possibility that he was being contacted to leverage his access to privileged information.

Jack ceased communication with the consulting company and revised the level of detail available on the professional networking site. Jack also advised his agency security adviser and submitted a report to the Contact Reporting Scheme. Further investigation identified the consulting firm was actually linked to a foreign intelligence service.

What if?

What would have happened if Jack hadn't dropped contact and reported it?

If Jack hadn't broken his contact with the consulting company, it's likely this would have matured to a relationship where Jack would have been given tasking to complete. Such tasking often begins with something benign, such as writing a report on readily available material, before escalating to tasking that requires the input of sensitive or privileged information. If Jack had undertaken this tasking, even if the material had not been national security classified, he could have been subject to a range of actions; from losing his security clearance and government employment through to prosecution under Part 5.2 (Espionage and related offences) of the Criminal Code.

What would have happened if Jack had dropped contact but hadn't reported it?

If Jack had broken his contact with the consulting company, but not reported it through the formal mechanisms, other less-aware individuals could have fallen victim to this targeting. Further, if Jack's contact with an entity of concern had been identified without Jack having reported it, this may have had an adverse impact on Jack's ability to maintain his clearance.

What happened after Jack reported the contact?

Because Jack dropped the contact and reported it, this provided assurance about his suitability to maintain his clearance. His agency security adviser was able to issue a circular advising other staff of the potential to fall victim to this type of targeting, and two other staff members came forward with remarkably similar experiences. Other Australian agencies were able to use the information provided to the Contact Reporting Scheme to warn other potential Australian victims.

For more information, talk to your security manager/adviser or visit:

www.asio.gov.au
www.cyber.gov.au

Recognise
the profile?

Realise
the potential threat

Report
to your security manager/adviser

Remove
them from your network