Australian Government

Australian Security Intelligence Organisation

ASIO

Think before you link

Guide for organisations

Introduction

Malicious social media profiles pose a risk to your staff, your organisation and national security. To support you in defending against this threat, we are running a campaign—'Think before you link'—which educates people about malicious profiles and how to respond to their approach.

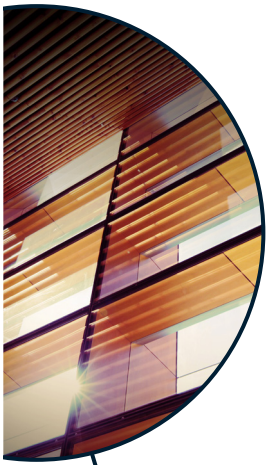
The impact of behaviour change campaigns of this kind relies very much on the planning and evaluation activities that each organisation sets in motion.

This guide will provide you with information about the threat of malicious profiles, the aims of the campaign, and the Five Es Behaviour Change Framework supporting the development of the campaign.

Then, it will outline the process of running the campaign in three distinct phases:

- activities we recommend you engage in before the campaign starts;
- activities we advise you engage in during the campaign; and
- actions you should take after the conclusion of the campaign.

“This guide is intended to support you in implementing the security campaign “Think before you link” in your organisation in the most effective way.”



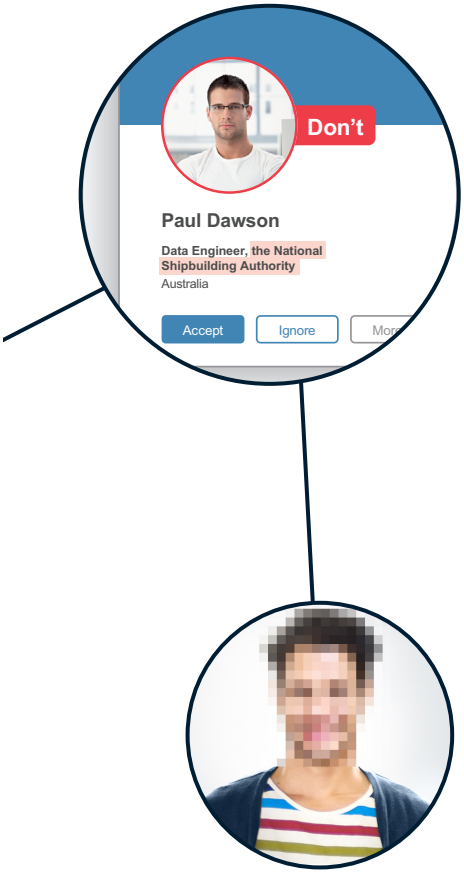
The threat

What's the problem?

Malicious actors are using professional networking sites and social media platforms to approach Australian and Western nationals working in sensitive employment across government, the private sector, academia and think tanks. These malicious actors piece together information from multiple sources to draw meaning from their intelligence gathering.

Why are they doing this?

Their goal is to recruit Australian and Western nationals who can provide them with sensitive intelligence, willingly or unwittingly. In the latter case, individuals may not recognise that the information they are providing is sensitive (for example, they may be asked seemingly benign questions).



Who are they targeting?

Individuals are particularly vulnerable to approaches if they include the following details on their profile:

- identify as an employee of the **Australian Government**;
- identify as working in the private sector or academia, **with access to classified or commercially sensitive technology or research**, either directly or indirectly (for example, the defence industry); or
- mention that they have a security clearance.

How do they trick you?

Typically, malicious actors contact the target posing as an interested 'employer' or recruitment consultant presenting **a unique business opportunity**. They ask for further details about the target's background, try to 'sell' the business opportunity, and insist on discussing it privately, away from the initial website. This kind of engagement is an attempt to understand the level of access the individual has to sensitive information, draw it out from them, and build a longer term relationship.

The aims of the campaign

The campaign ‘Think before you link’ aims to:

- raise awareness of the threat and educate clearance holders to understand the signs of a malicious approach online;
- provide people with a simple to-do list which motivates them to be vigilant and take action, through the four Rs:

Recognise
the profile?

Realise
the potential threat

Report
to your security manager/adviser

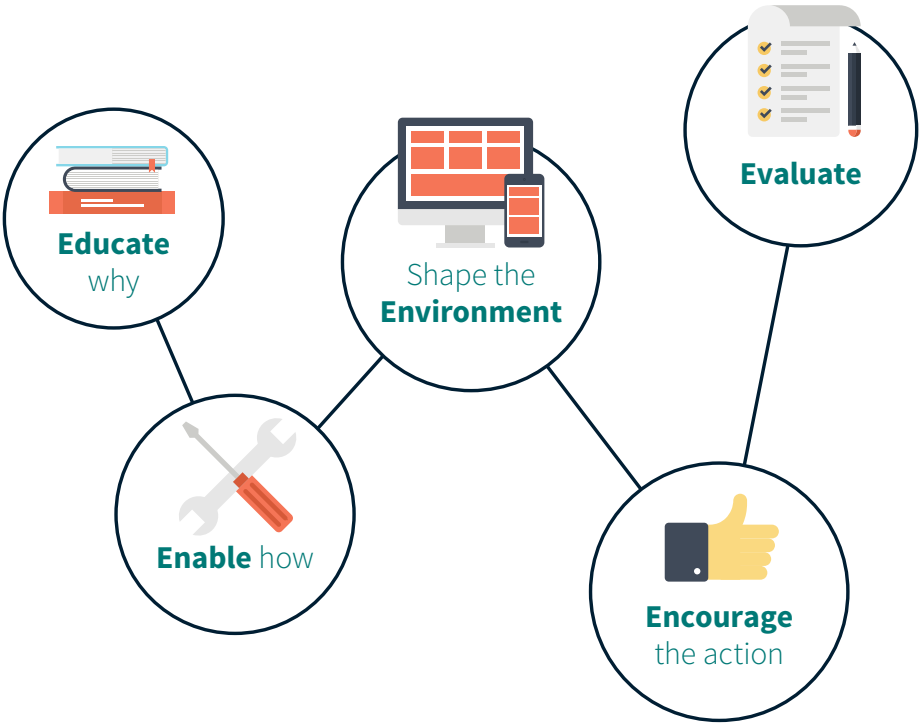
Remove
them from your network

- help them avoid being targeted in the first place; and
- deter malicious actors from using professional networks and other online platforms to target your staff.

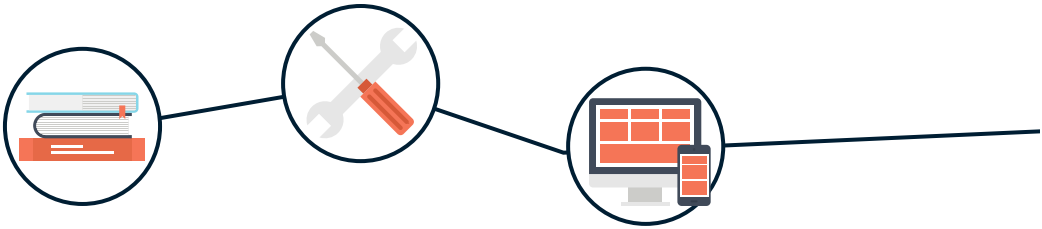
How to change behaviours

To deliver sustainable organisational behaviour change, there are five underpinning principles which serve as a checklist of what needs to be in place.

The Five Es Behaviour Change Framework is key to the success of every campaign and is made up of five principles:



The Five **E**s Framework



Educate why

People are more likely to engage in behaviour if they understand why it is important to do so. Educating means helping staff to understand the nature of the threat, and why this poses a risk to them, their organisation and national security.

Enable how

To behave in the desired way, staff need the necessary resources. In this context, they need clear, concise instructions on how to identify a malicious profile and what to do when they are approached by one.

Shape the **Environment**

Environmental cues can make it easier to do the right action, so it's important to shape the environment and ensure that the desired behaviours are as easy as possible for staff to do. In this campaign, this might involve reshaping reporting mechanisms so that they are streamlined and easy to use.

Underpinning the Five Es is the principle of endorsement. This proposes that the first four principles have more impact when augmented by the presence of credible sources who visibly endorse the messages in the campaign.

Encourage
the action

Staff need feedback to help reinforce the desired behaviour and discourage the undesired ones. If staff receive little or no meaningful feedback in response to their reporting, they may feel ignored and associate this behaviour with a negative experience. This could make them less likely to report again.

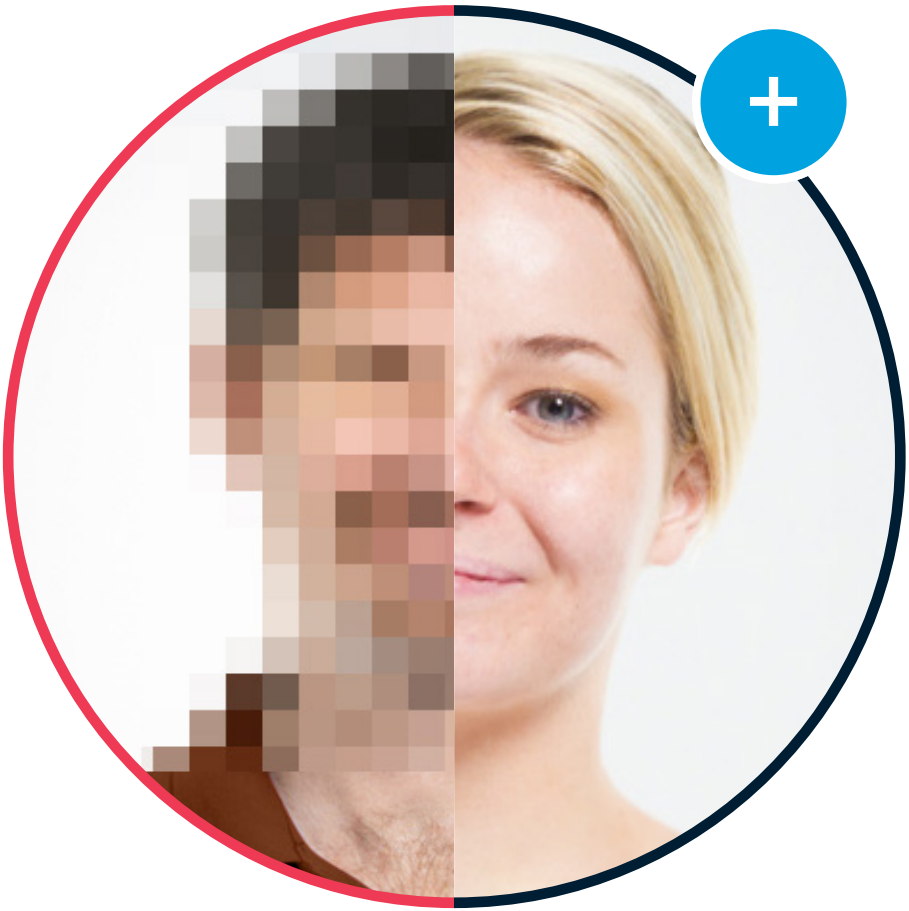
Evaluate

Like all change initiatives, assessing the impact of your campaign is an important step. Demonstrating the impact of the work will help raise support for future initiatives.

Pre-campaign activities

To get the most out of this campaign, there are a number of activities you should engage in before you start.

- Develop an implementation plan
- Gain support and buy-in from relevant stakeholders
- Review existing reporting mechanisms
- Conduct baseline activities



Develop an implementation plan

A strategic approach to implementing the campaign is extremely important. Early in the planning process you should:

- gather resources—assemble a small team who will manage the project;
- formulate goals—understand and clearly articulate what you hope to achieve by running the campaign;
- identify stakeholders—outline the individuals who can make or break the success of the campaign; and
- write a project plan—identify the key actions you need to take in order to deliver the aims of the campaign, when they must be done by, and who is responsible for them.

Gain support and buy-in

After identifying your key stakeholders, you might need to do some work to get those people on board with running the campaign.

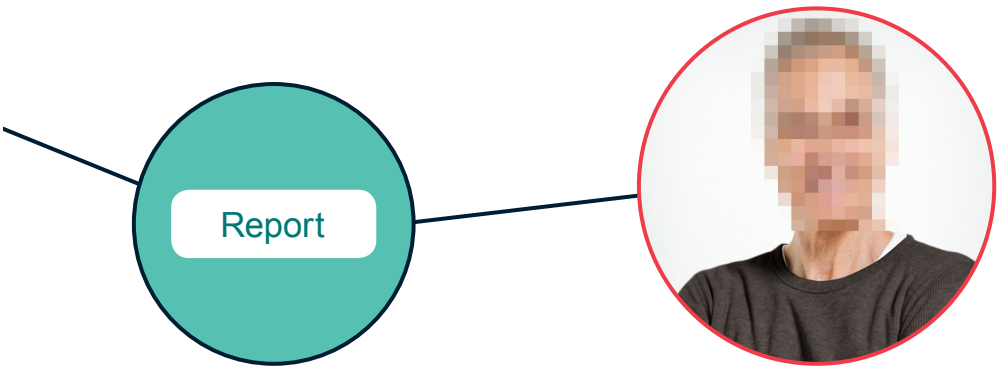
To support you in doing this, the campaign pack includes pre-prepared briefing notes. You can use them to discuss with stakeholders the aims of the campaign, the resources needed to run it, and the benefits you stand to gain. The briefing packs can be customised, so you can tailor the content to your specific audience.

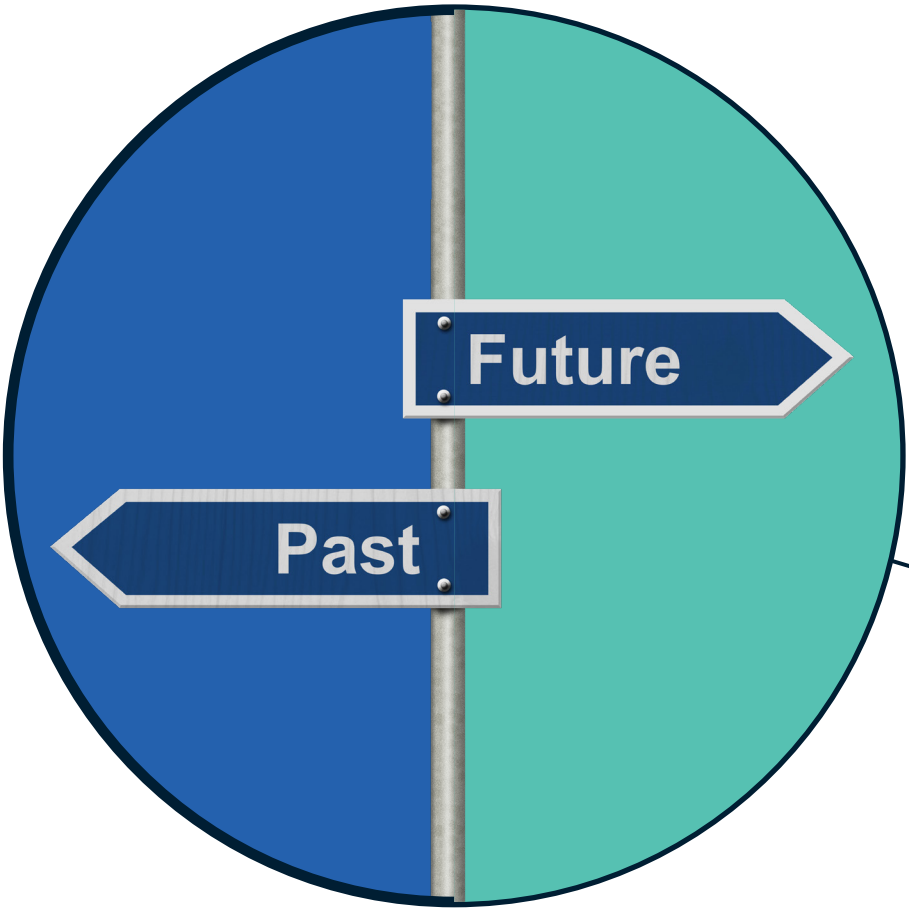
Review reporting mechanisms

One of the key aims of the campaign is to encourage people to effectively report approaches from the potential malicious profiles they encounter.

In order to do this, you may want to reshape your reporting mechanisms to make this process more accessible for your staff. It's important that this is done before the campaign, so that the message you communicate about how to report is clear and consistent.

Perhaps you don't have a formal procedure for this in place already, or the existing process does not support staff in engaging with it. A key first step is to review your current mechanisms for reporting on this issue.




Future
Past

Conduct baseline activities

After running the campaign, you will want to measure its impact on your staff's awareness and behaviour. So, ahead of the campaign, you should identify the means by which you'll assess your results. This will give you a baseline against which you can compare the campaign's final outcome.

You can do this by:

- identifying key sources of data—consider the information you already collect that might be useful for understanding staff attitudes or behaviour in relation to malicious approaches (for example, reporting statistics, security forums); and
- gauging staff attitudes using surveys or focus groups.

Campaign implementation

This section discusses the implementation of the campaign and the additional activities which can maximise its impact.

Campaign materials

The campaign pack includes a suite of materials to support you in communicating key messages to staff. The materials draw on the central theme of 'Think before you link' as the main call to action for staff. All the materials are designed to reinforce this message, remind staff about the nature of this threat, create a sense of excitement around the campaign, and elicit other key actions (such as removing malicious approaches or emails from networks).

The materials are:

- Guide for organisations
- Senior managers and security manager/ adviser briefing pack
- Online networking guide
- Staff briefing pack
- Case study
- flyer
- poster sets
- wallet cards

Support with communications

Guide for organisations

This booklet is aimed at security managers/advisers. It contains key guidance on how to implement the security campaign ‘Think before you link’ in the most effective way.

Senior managers and security manager/adviser briefing pack

This document will be used in initial face-to-face briefings to fully introduce the ‘Think before you link’ campaign to senior managers and security managers/advisers.

Online networking guide

This booklet is aimed at staff. It contains key guidance on how to spot malicious approaches and what to do when they encounter one.

Staff briefing pack

This document will be used in initial face-to-face briefings to fully introduce the ‘Think before you link’ campaign to staff.

Case study

This document contains stories of employees who've been targeted and exploited in the past.

Flyer

This document summarises the key points from the 'Think before you link' campaign.

Posters

These posters are designed to act as a reminder of the key messages and raise awareness about the campaign. The poster themes pick up on the main indicators of malicious profiles online and the main calls to action.

Reminder wallet cards

Working in conjunction with the other materials, these can be handed out to staff after face-to-face briefings, or desk-dropped to create further excitement about the campaign.

Provide briefings

Face-to-face briefings with staff are a good way to educate them about the threat, so they can understand why it's important to take steps to protect themselves and their organisation. If resources are limited, identifying which audiences are the most important to reach can help you have a stronger impact.

You may wish to conduct your own assessment of who the critical audiences are. But some of the groups to include could be:

- **managers**—harnessing a network of managers is a powerful way to disseminate messages about the campaign. Managers might face questions about the campaign, so keeping them well informed helps to provide a consistent message across your organisation; and
- **security clearance holders**—these professionals are the most likely to be targeted by malicious actors. So, if resources are limited, focusing attention on these groups helps to heighten awareness and vigilance in your staff.

Shape reporting mechanisms

One of the key objectives of the campaign is to encourage staff to report malicious approaches through the proper channels. This is a critical aspect of the campaign for several reasons:

- Staff reporting helps your organisation to understand more about its potential vulnerabilities in a particular area, and highlights areas for improvement.
- Reporting suspected malicious approaches helps your organisation provide support to staff who may have been targeted.
- Potential malicious approaches are of interest to ASIO. Staff reporting helps in the gathering of important intelligence.

> **‘It is important that information is properly handed to your organisation’s security manager/adviser, who will then act accordingly, sharing that information with ASIO if appropriate.’**

The following factors can lower the barriers to reporting and encourage staff to report their concerns:

Clarity

Make it clear who to contact, and when. It's always better to have one clear point of contact for reporting unusual activity.

Simplicity

Make it easy and straightforward to report (for example, steering away from long forms).

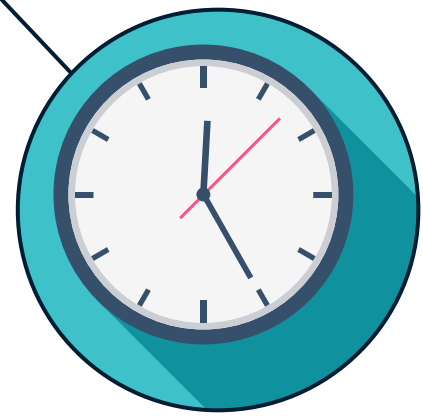
Confidentiality

Maintain confidentiality throughout the process, and be seen to be doing this. If a report leads to an investigation or disciplinary action, care should be taken to maintain the privacy of the staff involved, whenever possible.

Timing and responsiveness

Acknowledge receipt of concerns, explaining next steps and providing feedback where possible (or at least confirming that the report has been received and will be actioned, and thanking the reporter for submitting it).

Your organisation may also benefit from sharing with your staff some general information about the consequences and impact that reporting has had. Demonstrating that reporting has impact can increase similar behaviour.



Post-campaign actions

After running the campaign, there are still some activities that can help you make its impact as positive as possible. You can evaluate the campaign's results, reflect on the lessons learned and provide ongoing support.

Evaluate campaign impact

As with all change initiatives, it's important to assess the impact of the campaign and evaluate whether it has achieved its aims. Information gathered in the evaluation phase may help in assessing what ongoing work is required (for example, refresher training, or measures that target specific areas of the organisation).

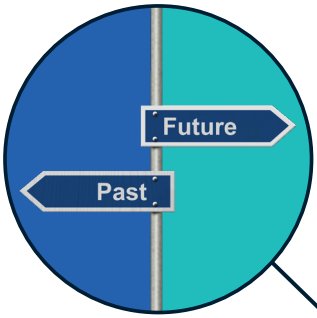
During the baselining phases, you should have identified some key metrics or data that you can use to assess change over time and evaluate the impact of the campaign. Revisit those data sources a predetermined period after the campaign to identify trends or changes in the data. Consider which other factors could have affected the relevant metrics, and bear their influence in mind.

Also, you may wish to communicate these final results back to the stakeholders, including staff, senior managers or specific people involved in running the campaign. Letting them know that your organisation is investing in following up on these initiatives will increase support for future campaigns.

Assess reporting mechanisms

Reporting is a key desired outcome of the campaign. If you made any significant changes to your reporting mechanisms before the campaign, conducting a brief review of their effectiveness can be very helpful.

Summary



Pre-campaign

- Gain support and buy-in
- Plan the program
- Review reporting mechanisms
- Conduct baseline activities

Campaign implementation

- Use the Five Es to change behaviour
- Use the campaign materials
- Provide training and briefings
- Tailor the campaign to your organisation

Post-campaign

- Evaluate impact
- Reflect on lessons learned
- Provide ongoing support

Example of a campaign roll-out

The specifics of how you deploy the campaign in your organisation will depend heavily on your aims for the campaign, the structure of your organisation, and the target audiences you are trying to reach. The table below provides a rough example of what a typical campaign roll-out might look like. Time frames will vary from one organisation to another.

Pre-campaign 4–6 weeks		**Live campaign** 12 weeks		**Post-campaign** 4 weeks after campaign	
Activities	**Resources**	**Activities**	**Resources**	**Activities**	**Resources**
Engage stakeholders	Senior managers briefing pack	Provide briefings to key staff	Staff briefing pack	Evaluate reporting statistics	Organisation guide
Gain senior management buy-in	Organisation guide	Provide communications from senior figures/relevant experts	Posters	Conduct post-campaign surveys or focus groups	
Develop a communication plan		Launch poster materials	Staff guide	Monitor other feedback channels	
Prepare or adapt materials		Embed briefings and materials into existing delivery mechanisms (e.g. induction for new starters)	Flyer	Maintain and update campaign materials for ongoing security briefings (e.g. induction, leavers)	
Review reporting mechanisms			Case studies		
Conduct baseline evaluation metrics			Supporting materials		

Other resources

The ‘Think before you link’ campaign materials have been designed to help organisations raise awareness of the threat posed by malicious approaches and encourage behaviour change to mitigate the potential impact of these hostile actors. It is also important to consider other resources that might help to secure your organisation and protect staff from this threat and others like it. Physical and cyber security measures should be employed in combination to keep your organisation secure.

For more information:

www.asio.gov.au

www.cyber.gov.au