Think before you link

Guide to running an effective ‘Think before you link’ campaign

PSR | Protective Security Requirements

About this guide

Malicious online profiles pose a threat to your organisation's people, information, assets, and work locations. They can also threaten national security. The 'Think before you link' campaign is designed to help your organisation recognise and respond to this threat.

This guide shows you how to plan and implement an effective awareness campaign.

Behaviour change campaigns of this kind rely on putting in place effective planning and evaluation strategies.

This guide will provide you with the tools to help your colleagues understand the threat posed by malicious online profiles and lays out a programme framework to help you change behaviours in your organisations.

We also show you how you can sustain interest in your campaign by taking a planned and deliberate approach and suggest ways to track whether the message has got through.

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

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

We want to help you spread the word about 'Think before you link' so you can run the most effective security campaign possible.

Understand the threat

What is the threat?

Malicious individuals, and groups such as foreign state actors and criminals use social and professional networking sites to target and exploit people who may have access to sensitive or valuable information and resources.

What are their motives?

People who use malicious online profiles aim to exploit their targets for criminal, social, economic, or political gain. Because it's easier to disguise their true identity and intentions online, this kind of deception is a useful tool for foreign state actors and criminals alike. Their goal is to recruit targets and get them to provide sensitive or valuable information.

Who do they target?

Malicious actors look for people with high status positions who may have access to valuable information or resources.

Your people are at greater risk of being targeted if they:

- disclose that they have access to classified or commercially-sensitive information, technology, or research
- reveal they have a national security clearance.

How do they trick their targets?

Malicious actors often appeal to their target using flattery or by offering something valuable. They'll then try to build rapport with their target. Developing a long-term relationship gives them more opportunity to manipulate their target into giving away sensitive information (willingly or unwittingly, and sometimes in exchange for rewards).

Foreign state actors and criminals often pose as employers or recruitment consultants. They'll try to present their target with a unique business or career opportunity. Under this guide, they may ask for more details such as their exact role within your organization as they try to find out if they have access to sensitive information. The target may not realise the information they share is sensitive and just feel that they are responding to a legitimate business or career opportunity.

Aims of the ‘Think before you link’ campaign

This campaign aims to help everyone at your workplace to:

- recognise the warning signs of a malicious online profile
- know what to do if a malicious actor targets them
- know how to avoid being targeted in the first place
- deter malicious actors from using professional networks to target your organisation.

The campaign offers a simple approach to managing this threat using the ‘4Rs’:

Recognise
a suspicious profile

Realise
the potential threat

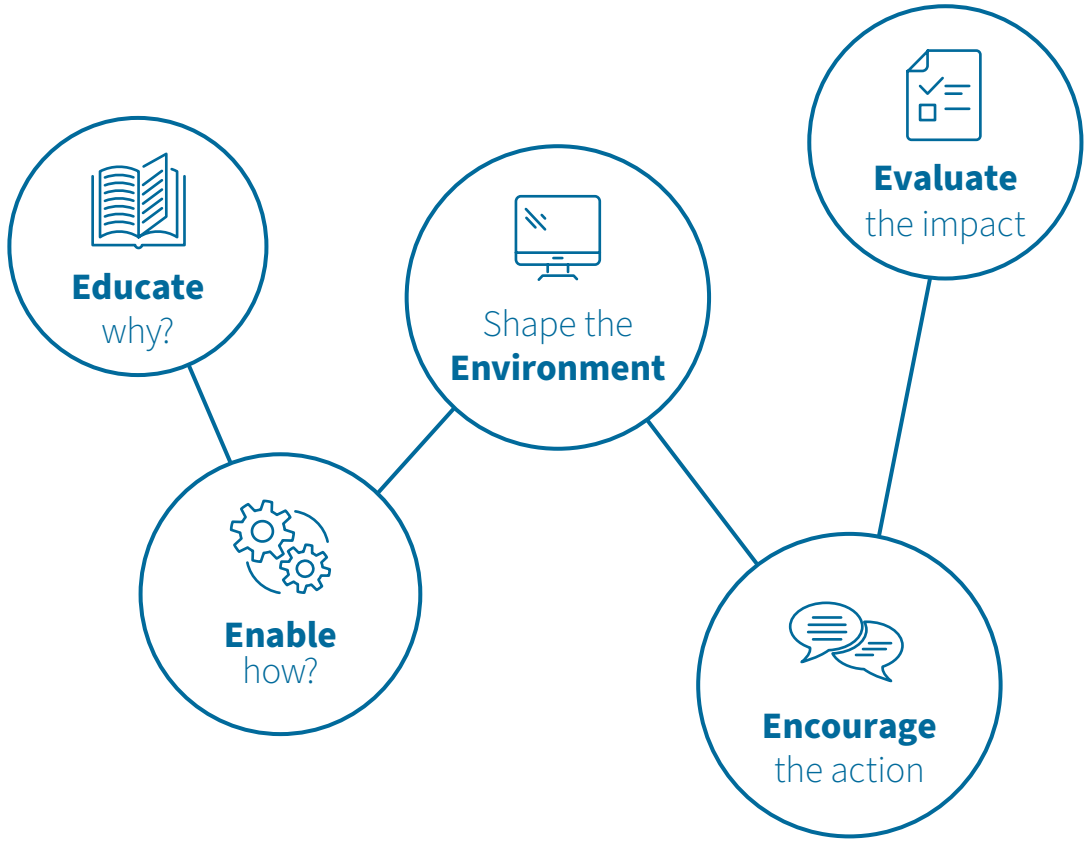
Report
your concerns

Remove
them from your network

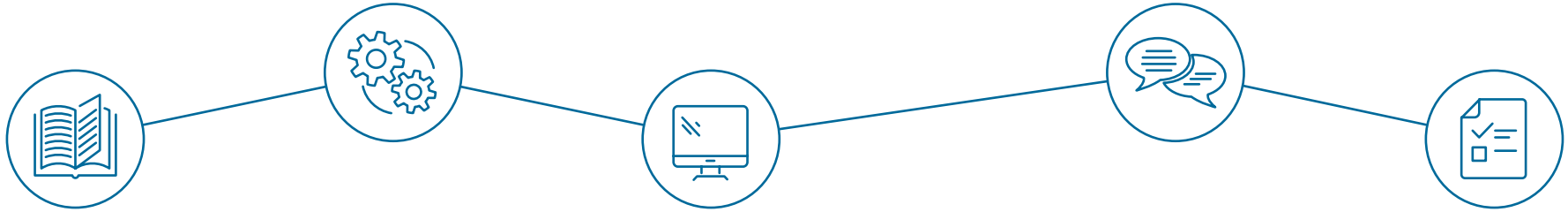
Change behaviours

This campaign is built on the 'Five Es behaviour change framework', which is underpinned by five main principles. Follow the stages of the framework and apply the principles to help you to change behaviours and make those changes stick.

The Five Es framework and its principles are the foundation for a successful campaign.



Follow the Five Es framework



Educate – why?

People are more likely to adopt the right behaviour if they understand why it's important to do so. Educate everyone about the nature of the threat and the risks it poses, so they understand why they need to protect themselves. They'll also understand the wider implications for protecting their organisation's people, information, assets, and work locations.

Enable – how?

Teach all employees how to identify a malicious online profile and what action to take if they encounter a suspicious approach. Make sure your instructions are clear and concise, and any processes are easy to follow.

Shape the **Environment**

Create an environment that makes it easy for your people to act when they encounter a threat. Ensure your reporting mechanisms are streamlined and easy to use. Foster a culture that is non-discriminatory and proactive.

Encourage the action

Give people meaningful feedback that reinforces the desired behaviour. If they report a threat, give positive feedback that rewards their action. If you see or hear of undesirable behaviour, educate the person and encourage the right action.

Evaluate the impact

Assessing the impact of the campaign is important. Decide how you will measure success and raise support for future initiatives.

Seek endorsement from your senior leadership team

The first four principles will have more impact if your senior leadership team visibly endorses the campaign.

Prepare for the campaign

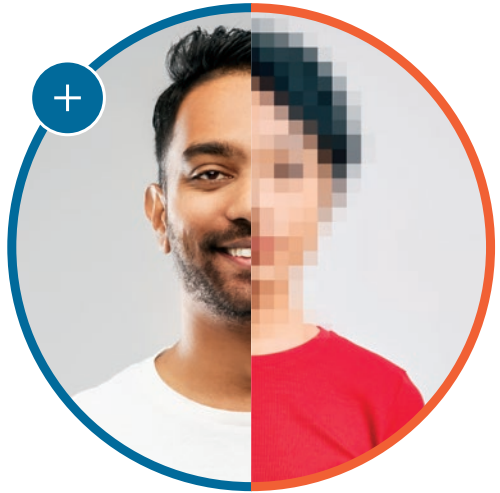
To ensure your organisation gets the most out of the campaign, you'll need to be well prepared.

- Develop an implementation plan
- Gain stakeholder support
- Review your current reporting mechanisms
- Set a baseline to measure success against

Developing an implementation plan

Take a strategic approach to implementation to help your campaign succeed. You should complete to following tasks early in the planning process.

- **Gather resources.** Assemble a team to manage the project
- **Set goals.** Understand and clearly articulate what you hope to achieve from the campaign
- **Identify influential stakeholders.** Know who can make or break the success of the campaign
- **Write a project plan.** Identify the key action steps for running the campaign successfully



Review your current reporting mechanisms

One of the key aims of the campaign is to encourage people to report suspicious approaches they encounter online. You'll need to make sure it's as easy as possible to raise concerns.

Review your current reporting mechanism to ensure the right policies, procedures and systems are in place. If they're not, you'll need to get your processes in order before your campaign begins.

Report

Set a baseline to measure success against

Identify how you will measure the success of your campaign before you begin. Once you are underway, you'll want to know how it's impacting awareness and behaviours.

Some ideas to get you started

- Identify key sources of data: what information do you already collect that might be useful for understanding people's attitudes or behaviour towards malicious profiles? For example, check past statistics and results of previous security forums.
- Gauge staff attitudes using surveys or focus groups.

Implement the campaign

In the implementation phase, make use of the supporting materials and carry out some additional activities to help you maximise the campaign's impact.

Use the supporting materials in your campaign

This campaign comes with supporting materials to help you communicate the key campaign messages to people in your workplace.

The materials reinforce the central message of the campaign (Think before you link). They're designed to remind everyone about the nature of the threat, create a buzz around the campaign, and bring about other key actions (such as removing malicious profiles from networks).

The materials are:

- Guide to running an effective 'Think before you link' campaign
- A guide to networking safely online
- Online networking – a guide to recognising when an online profile is malicious
- Case Studies based on real examples of malicious online profiles

Supporting materials

Guide to running an effective ‘Think before you link’ campaign

The booklet you are currently reading presents advice on how to implement the ‘Think before you link’ campaign in your organisation. Share it with your project team.

A guide to networking safely online

This educational booklet will help people in your organisation to identify a malicious profile and tell them what to do if they encounter a suspicious approach online.

Online networking – a guide to recognising when an online profile is malicious

This short and informative pamphlet outlines how to recognise a suspicious profile or when an online approach might be malicious.

Case Studies based on real examples of malicious online profiles

The case studies include examples of people who have experienced suspicious online approaches or fallen victim to malicious profiles and targeted exploitation.

Hold briefings to reach key people

Face-to-face briefings are a good way to inform people about the threat of suspicious approaches and teach them what to do if they encounter a malicious profile.

If your resources are limited, identify which groups of people are the most important to reach. Consider holding briefings with the following groups of people to strengthen your campaign's impact.

- Managers — harnessing a network of informed managers is a powerful way to spread the campaign messages. Managers need to be well informed because they'll be the first point of contact for questions from their teams. Briefing managers will also help you to ensure the campaign messages are consistent across your organisation.
- National security clearance holders
- Individuals or groups with access to controlled information or to commercially-sensitive information, technology, or research
- Individuals in positions of influence
- Areas of your organisation that have experienced or fallen victim to malicious profiling
- Security personnel

Shape reporting mechanisms to support your campaign

One of the key objectives of the campaign is to encourage people to report suspicious encounters through established processes and channels.

This objective is critical for several reasons. When it's easy for everyone to report malicious approaches or suspected ones, it helps your organisation to:

- understand more about its potential vulnerabilities and highlights areas for improvement
- provide support to people who may have been targeted
- ensure that reports reach the right people, so the most appropriate action can be taken
- potential malicious profiles could be of interest to your security teams. Staff reporting helps in the gathering of important intelligence.

It's important that information is reported to the security team in your organization, who will then assess how it is shared.

Good reporting mechanisms will encourage staff to speak up

Clarity

Be clear about who to contact and how. It's always better to have one clear point of contact for reporting unusual activity.

Simplicity

Make reporting as easy and straightforward as possible. For example, steer away from long forms and instead create a simple electronic template or a portal in your organisation's intranet.

Confidentiality

Maintain strict confidentiality of the information reported and provide regular reassurance privacy will be respected at all times.

Responsiveness and timing

Always promptly acknowledge any reports you receive so people know that action is being taken. Thank them, explain the next steps, and provide feedback that reinforces best practice. Consider sharing general information about the impact of reporting, so people who've reported know they've made a difference and others are encouraged to follow suit.

Evaluate the campaign

After you've run your campaign, make sure you reflect on the lessons learned.

Evaluate the campaign's impact

With all change initiatives, it's important to evaluate the campaign's impact so you know if it's been successful.

Use key metrics and data to assess the impact of your campaign. Analyse the information and review your findings. Consolidate your results and produce a report that summarises the outcomes of the campaign.

You may wish to share your findings with people who supported the campaign. Feedback is a powerful tool for motivating change and will increase support for ongoing work and future initiatives.

Information you gather in the evaluation phase may also help with assessing what ongoing work is required. Will people need refresher training? Will you need measures that target specific areas of the organisation?

Assess your reporting mechanisms

The ability to report suspicious profiles and online approaches is the key deliverable from the campaign. Review the effectiveness of your reporting mechanisms. Did your reporting mechanisms work well? Did you make changes to any existing process you had in place? If so, what new mechanisms did you implement? How effective were these changes? And what recommendations would you make for the future?

Summary of the campaign phases

Incorporate the Five Es framework in all the campaign phases to increase awareness and lift capability.

Preparation phase

- Plan the campaign around the results you want achieve
- Gain support from key stakeholders
- Review your current reporting mechanisms
- Set a baseline for measuring success against

Implementation phase

- Use the campaign materials to spread the campaign's messages
- Hold briefings to train people and get them on board
- Shape reporting mechanisms to support your campaign

Evaluation phase

- Evaluate the impact
- Share lessons learned with key people
- Decide what ongoing support to provide
- Assess your reporting mechanisms

Consider using other resources

The ‘Think before you link’ campaign materials aim to raise awareness of the threats posed by people who create malicious profiles. This raised awareness helps organisations to mitigate the risks of harm to their people, information, assets, and work locations.

Recognise
a suspicious profile

Realise
the potential threat

Report
your concerns

Remove
them from your network

PSR | Protective Security Requirements

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