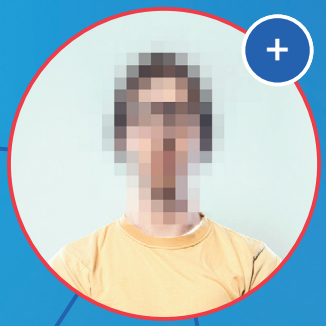


Think before you link

Guide for organisations

CPNI
Centre for the Protection of National Infrastructure

Branding

Crown copyright

Introduction

Malicious profiles pose a risk to your staff, your organisation and national security. To support you in defending against this threat, we have developed a campaign – Think before you link – which educates people about malicious profiles and how to react to their approach.

The impact of behaviour change campaigns of this kind relies very much on the planning and evaluation activities that every organisation sets in motion. CPNI has a track record of supporting organisations in the running of these campaigns and initiating changes that "stick".

The guide will initially provide you with relevant 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 before the campaign starts
- Activities we advise during the campaign
- 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"**

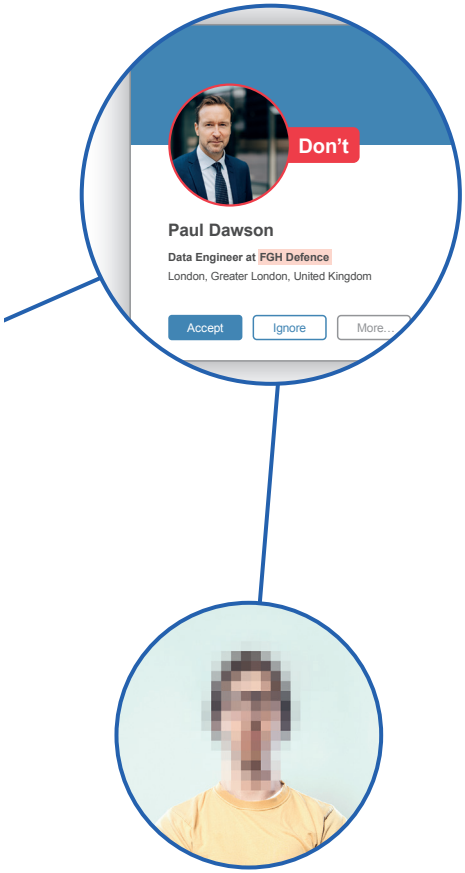
The threat

What's the problem?

Hostile actors and **criminals** are known to be using professional networking sites and social media platforms to approach UK 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 end goal is to recruit UK and Western nationals to provide them with sensitive intelligence, willingly or unwittingly. In these cases, individuals may not recognise that the information they are providing is sensitive (e.g. 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:

- Identifying as an employee or member of **HMG or Civil Service**
- Identifying as working in the private sector or academia, **with access to classified or commercially sensitive technology or research** either directly or indirectly (e.g. the defence industry)
- Mentioning that they have **security clearances**, especially security cleared (SC) or developed vetting (DV)

How do they trick you?

Typically, hostile actors and criminals 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:

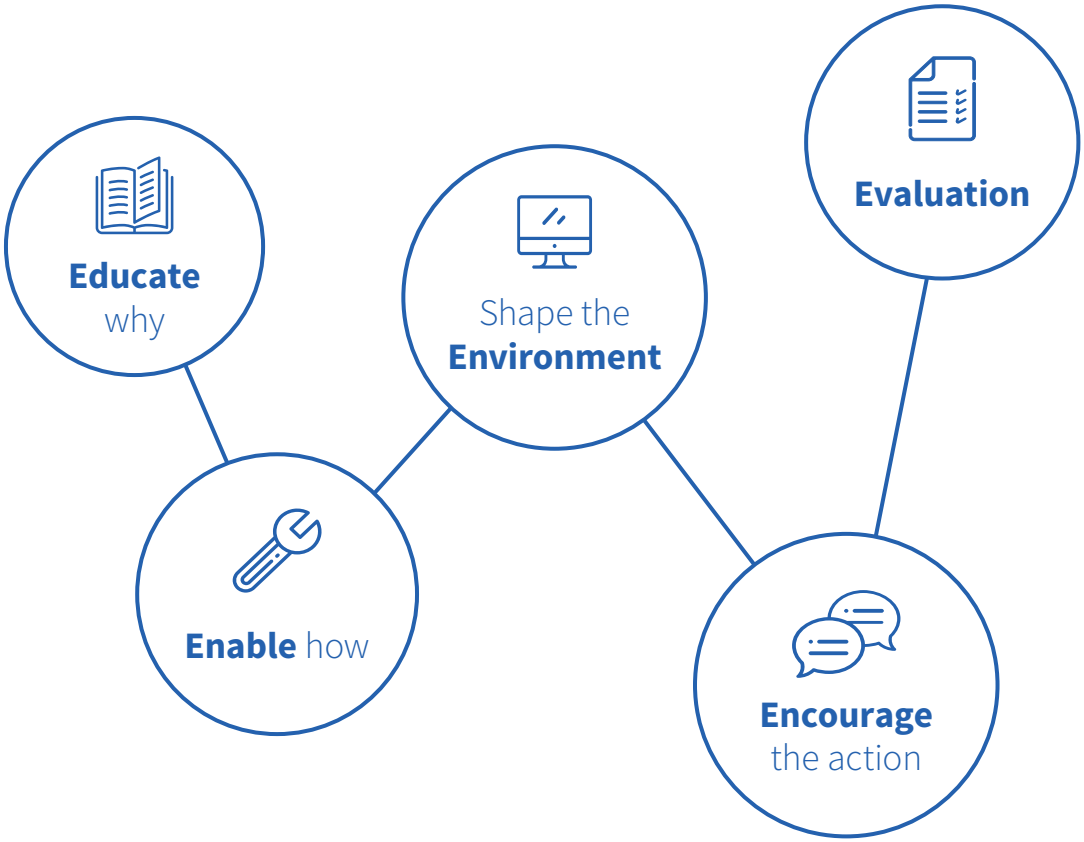
- Raise awareness of the threat and educate SC/DV cleared staff to understand the signs of a malicious approach online
- Provide people with a simple to-do list which motivates them to be vigilant and take action, through the 4Rs:

- Help them avoid being targeted in the first place
- Deter malicious profiles from using professional networks for targeting your staff

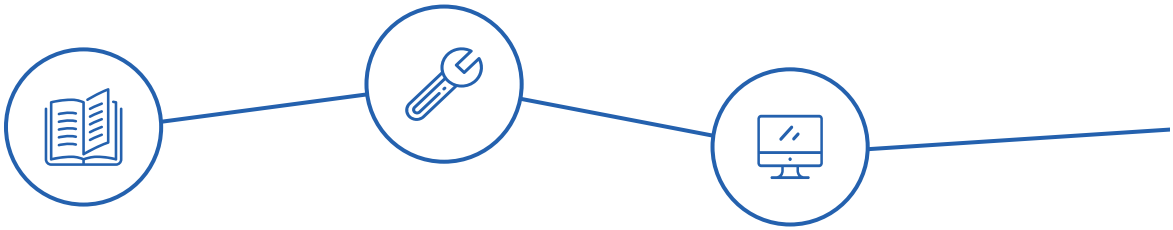
How to change behaviours

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 is about helping staff to understand the nature of the threat, and why this poses at risk them, the organisation and national security.

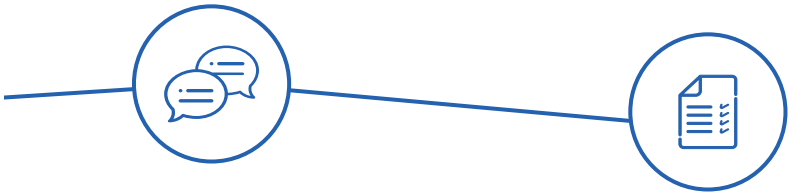
Enable how

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 re-shaping 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 are more impactful 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 one. 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.

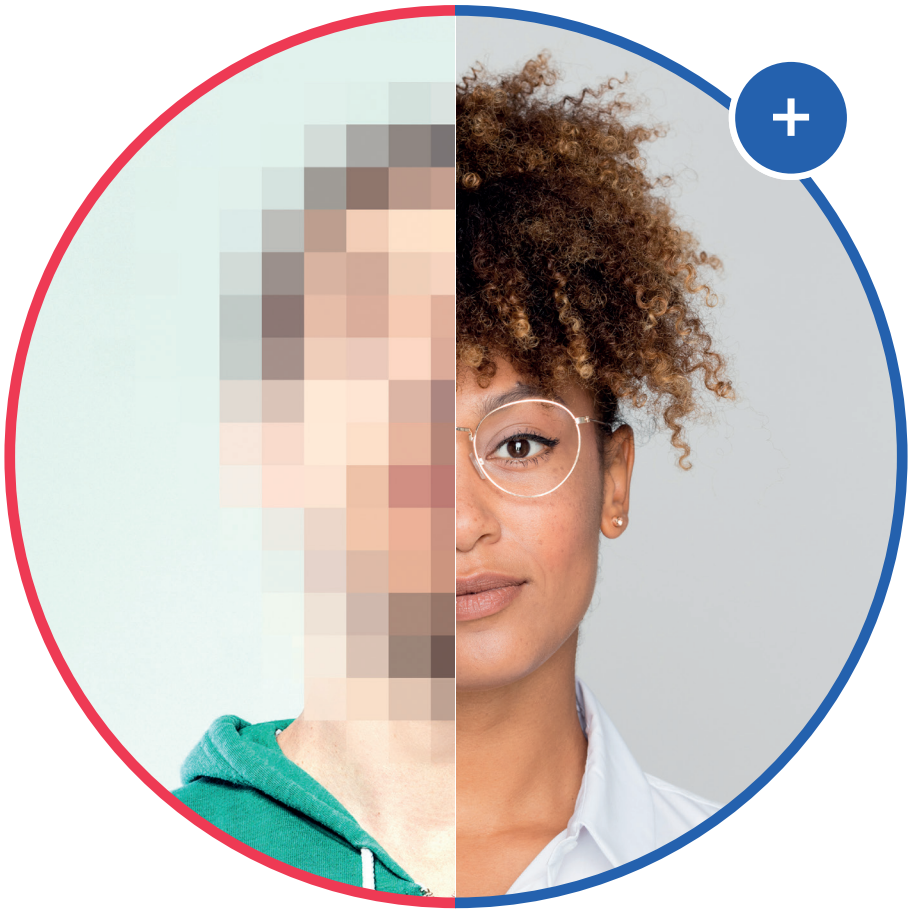
Evaluation

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.

- Developing an implementation plan
- Gaining support and buy-in from relevant stakeholders
- Reviewing existing reporting mechanisms
- Baselining



Developing 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 that can make or break the success of the campaign.
- Write a project plan – Identify the key actions you need to take in order to deliver the aims of the campaign, when by, and who is responsible for them.

Gaining 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.

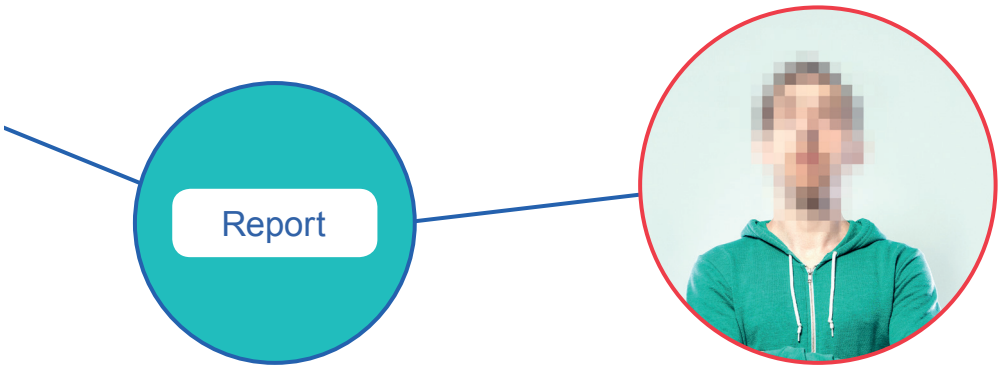
To support you in doing this, CPNI has created pre-prepared briefing notes. You can use them to discuss with stakeholders the aims of the campaign, the resources needed to run it, and the benefits you stand to gain. The briefing packs can be customised, so you can tailor the content to your specific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

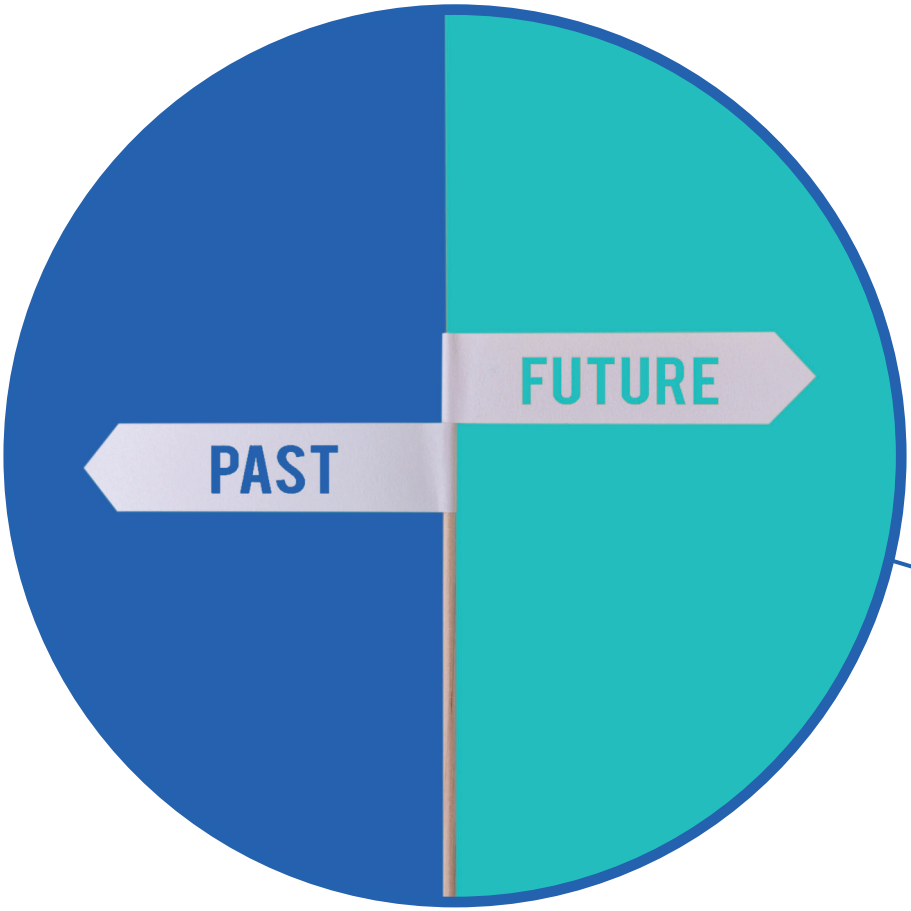
Reviewing Reporting Mechanisms

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 haven't got 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 a review of what your current mechanisms are for reporting on this issue.





Baselining

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 – what information do you already collect that might be useful for understanding staff's attitudes or behaviour in relation to malicious profiles? (e.g. reporting statistics, people groups, security forums).
- 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

CPNI has developed 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 buzz around the campaign and elicit other key actions (such as removing malicious profiles from networks).

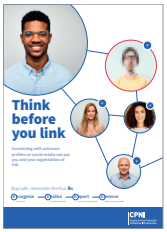
The materials are:

- Guidance for organisations
- Guidance for staff
- Poster sets
- Wallet cards
- Case studies
- Senior briefing pack
- Staff briefing pack

Supporting with comms

Guidance for organisations:

This booklet is aimed at organisations. It contains key guidance about how to implement the security campaign 'Think before you link' in the most effective way.



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.

Guidance for staff:

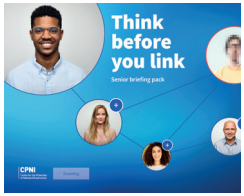
This booklet is aimed at staff.
It contains key guidance about how to spot malicious profiles and what to do when you encounter one.

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 buzz about the campaign.

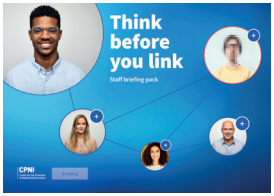
Senior briefing pack:

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



Case studies:

This document will contain stories of employees who’ve been targeted and exploited in the past.



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.

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 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.
- SC and DV cleared individuals – These professionals are the most likely to be targeted by malicious profiles. So, if resources are limited, focusing attention on these groups helps to heighten awareness and vigilance in your staff.

Shaping Reporting Mechanisms

One of the key objectives of the campaign is to encourage staff to report malicious profiles 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 profiles helps your organisation provide support to staff who may have been targeted.
- Potential malicious profiles are of interest to the security service. Staff reporting helps in the gathering of important intelligence.

> **“It is important that information is properly handed to departmental security officers, who will then act accordingly, sharing that information with the security service if appropriate.”**

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

Clarity:

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

Simplicity:

Making it easy and straightforward to report (e.g. steering away from long forms).

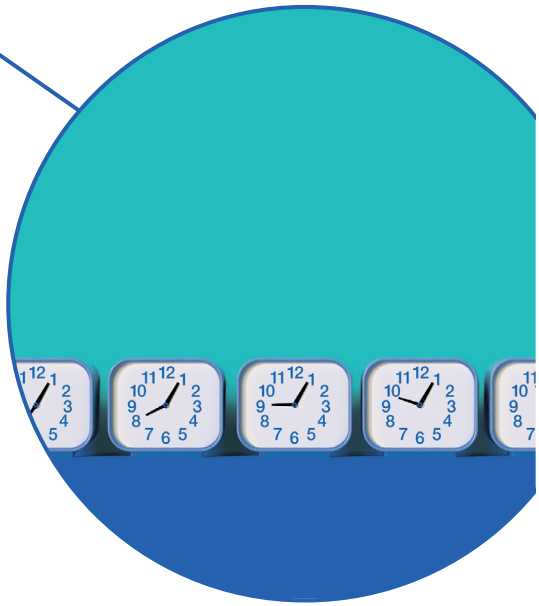
Confidentiality:

Maintaining confidentiality throughout the process and being seen to do 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:

Acknowledging 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 keep providing ongoing support.

Evaluating 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 (e.g. refresher training, or measures that target specific areas of the organisation).

During "baselining" 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.

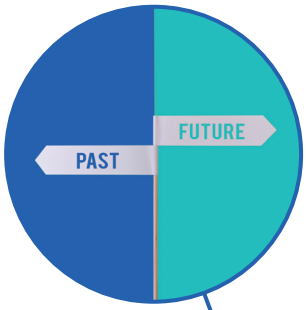
Assessing Reporting Mechanisms

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 programme
- Train consideration
- Baseline activities



Post-campaign

- Evaluate impact
- Lessons learned
- Ongoing support

Campaign Implementation

- Use the Five Es to change behaviour
- Use the campaign materials
- Training and briefing
- Tailor the campaign to your organisation

Example 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 below provides a rough example of what a typical campaign roll-out might look like. Time frames are based on typical examples from previous CPNI campaigns but will vary from one organisation to another.

Other Resources

The 'Think before you link' campaign materials have been designed to help organisations raise awareness of the threat posed by malicious profiles 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.cpni.gov.uk

www.ncsc.gov.uk

Pre-campaign 4-6 weeks		Live campaign 12 weeks		Post-campaign 4 weeks post-campaign	
Activities	**Resources**	**Activities**	**Resources**	**Activities**	**Resources**
• Stakeholder engagement	• Senior Briefing packs	• Briefings to key staff	• Staff briefing packs	• Evaluate reporting statistics	• CPNI Embedding Security Behaviours Using the 5Es
• Gain senior Buy-in	• Organisation guide	• Communications from senior figures/relevant experts	• Posters	• Post-campaign surveys or focus groups	• CPNI Guidance: Evaluation Guide for Internal Security Behaviour Campaigns
• Develop a communications plan	• CPNI Embedding Security Behaviours Using the 5Es	• Launch poster materials	• Staff guide	• Monitor other feedback channels	• Organisation Guide
• Prepare or adapt materials		• Embed briefings and materials into existing delivery mechanisms (e.g. new joiners)	• Flyer	• Maintain upkeep of campaign materials for ongoing security briefings (e.g. induction, leavers).	
• Review reporting mechanisms			• Case studies		
• Baseline evaluation metrics			• Supporting materials		

Crown copyright