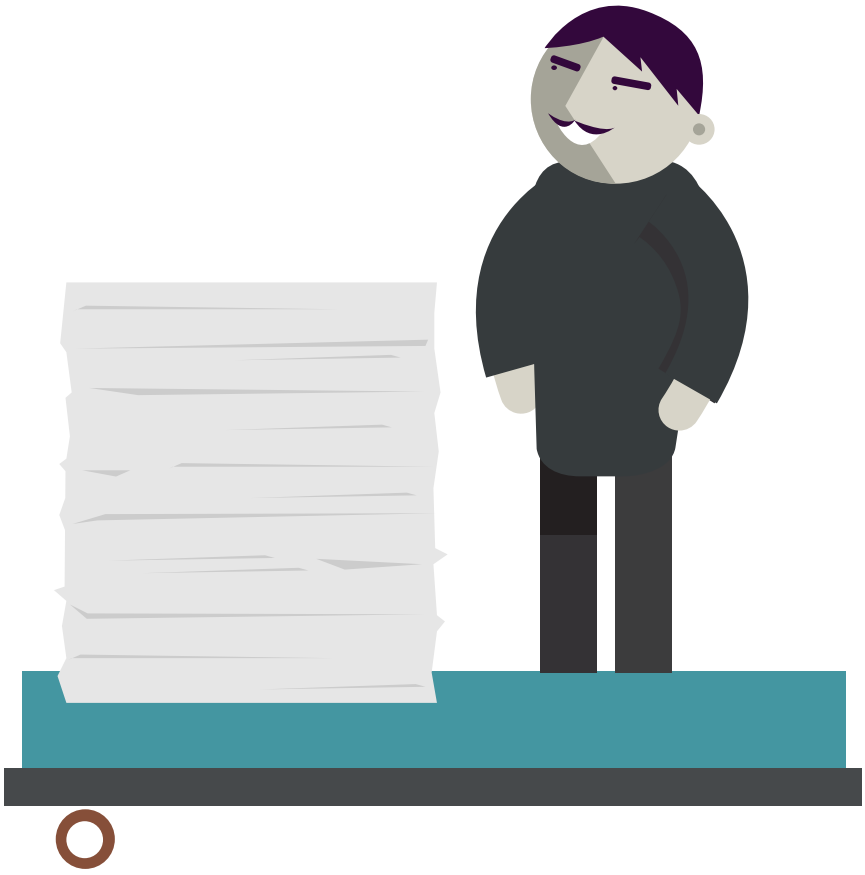
SOCIAL ENGINEERING CAMPAIGN STARTER KIT

CPNI
Centre for the Protection of National Infrastructure

DISCLAIMER

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it. This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at www.cpni.gov.uk.



INTRODUCTION

This campaign kit has been designed by CPNI to help you educate staff about social engineering. It aims to raise awareness about what social engineering is, what an approach might look like, and how staff can better protect themselves against this type of threat.

Different organisations may need staff to behave in different ways, depending on what's specifically at risk. But if you're stretched for resources, this easy-to-use kit offers practical security advice that everyone can follow, and the materials required to run a campaign.

It addresses six key issues. These are:

- Encouraging employees to use common sense when they come across something unusual or suspicious (e.g. an unusual telephone call, email, or social networking invite)
- Verifying the details of unknown suppliers or customers before disclosing organisational information
- Thinking about what information employees share outside of the organisation and whether this is too much
- Checking whether email addresses from unknown senders are genuine or bogus
- Being alert to phishing attacks and being careful not to click on malicious links or attachments
- Not being pressurised to make decisions when being put on the spot without first checking security policy

WHAT IS SOCIAL ENGINEERING?

Social engineering is the process of obtaining information from others under false pretences – in essence, manipulation. It is based upon the building of an inappropriate trust relationship with employees, and can be used against those within an organisation. For example, it could be an attempt to gain entry to a site or access to an organisation's IT systems using a bogus pretext.

A social engineer might choose to manipulate an instant rapport they've built with an employee, or build a longer-term relationship with them. They establish a level of trust so that the staff member feels comfortable to disclose information or grant the social engineer access without a second thought. It can happen to anyone and a staff member does not have to be particularly vulnerable. The important point about social engineering is that the organisation might well have sophisticated firewalls, good password protection and robust entry point procedures, but it's the human element that can be the weak point and potentially exploitable.

HOW TO RUN A SOCIAL ENGINEERING CAMPAIGN

This document outlines some key principles and guidance that should be followed when running a successful campaign. While CPNI has developed some materials to help UK organisations deliver a campaign, a detailed and coordinated campaign strategy will be required that is likely to encompass a campaign project plan, a staff communications plan and the development of additional supporting campaign materials (e.g. intranet articles by a senior manager and/or the security department).

The CPNI materials that have been developed are as follows:

- 1 x guidance booklet for staff called 'What is social engineering?' (this includes a short quiz for staff to complete at the end, to test their knowledge levels)
- 3 x posters that demonstrate different forms of social engineering
- 1 x video on social engineering
- 1 x checklist for staff on protecting themselves from the social engineering threat at work (e.g. for staff to pin near their desks)
- 1 x flier/desk drop to introduce the concept of social engineering to staff (e.g. perhaps to be used at the outset of the campaign)

You can see examples of these materials at the back of this guide in the Annex. These are also available to download from the CPNI Extranet as PDFs.

Some of the materials in the campaign kit are editable (using InDesign) to allow you to add your own organisational logo in place of the CPNI logo (e.g. the posters, checklist and flier/desk drop). To request access to these editable files, please email CPNI at PerSec@cpni.gov.uk

A) FIVE STEPS TO DELIVERING LASTING BEHAVIOUR CHANGE

Detailed below are five steps on how to make best use of these materials as part of a campaign to deliver lasting behaviour change in the workplace. Once you have digested these, you can take some practical measures to get your campaign up and running.

The first step is to educate staff on the role they play in security, and how their behaviour can help to detect and prevent social engineering attacks. Education, however, is just one part of a campaign to change security behaviours and embed security-savvy instincts. Follow the five 'Es' – your five steps to campaign success:

- Education
- Endorsement
- Ease
- Enforcement
- Evaluation

FURTHER INFORMATION ON EACH OF THESE IS DETAILED IN THE FOLLOWING PAGES.

1. EDUCATION

Motivation is fundamental to behaviour change. Unless employees understand the threats they and their organisation face from social engineering, and the fact that they have a role to play in combatting it, they will not be inclined to change how they act. Therefore educating staff about social engineering, its potential impact and the part employees play is critical.

There is a risk that staff can be complacent about threats and sometimes believe they have no contribution to make to their organisation's security. This complacency stems from a fundamental lack of awareness of the risk they themselves can pose to security.

However, while raising awareness of the danger is very necessary, remember to counterbalance this with reassurances about the training, support and measures you have in place to keep your people safe.

2. ENDORSEMENT

Having the right message, and medium to disseminate it, is only part of the story. You must decide who will be the 'voice' of your campaign. Who has the greatest credibility? Who will make the message really resonate with staff? At work, we're bombarded with requests to 'do this' and to 'do that'. So a successful campaign relies on having significant others from inside the organisation (or outside where appropriate) to tell staff about the social engineering threat and the importance of recognising it and reporting it.

Different staff audiences might need endorsement from different people. For example, if you have a cynical group of staff then you may consider that endorsement is best coming from a credible external expert. For new staff, attending their induction course, the message is likely best delivered by the head of security.

Regardless, the message should be endorsed from the top – through written communications and staff announcements from the head of the organisation.

The security manager, too, has a key role to play in reinforcing the message and communicating that they are the 'go-to person' for any reports of suspicious activity (see also 'Step 3. Ease' on page 6).

Think laterally about all the different occasions where the messages can be delivered and endorsed: for example, during induction, ongoing security training, staff get-togethers and staff review meetings.

3. EASE

If you want staff to be alert to the social engineering threat, then any action they're required to take should be as easy as possible for them to do. This means providing simple, clear and easy-to-understand guidance on what the social engineering threat is and what an approach might look like.

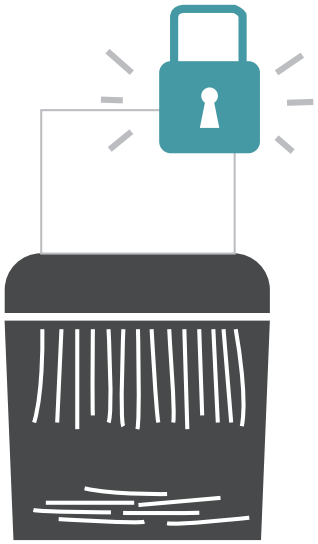
It also means providing some simple steps employees can take when they have concerns about being potentially socially engineered, such as how to respond and how to report suspicious behaviours back to security for further investigation.

A list of suspicious activities is really useful (our posters, videos and supporting materials can help). **For example:**

- Out of the ordinary requests for access to your organisation
- Emails from individuals or organisations you are not familiar with asking you to click on links or open attachments
- Approaches from individuals you are not familiar with outside of work who express excessive interest in a sensitive project in your organisation

Make sure that employees are empowered to challenge individuals who they believe are trying to socially engineer them. If your employees fear they will be criticised, teased or even punished for raising a concern with others, they are more likely to bypass or ignore security procedures.

Ensure the instructions for reporting a suspected social engineering threat are clear, and have them widely communicated throughout the organisation. Remember to emphasise that reporting will remain confidential and will always be taken seriously.



4. ENFORCEMENT

This 'E' is all too often forgotten. Behaviour change cannot rely on education alone; staff are human and bad behaviours can all too easily become the norm. Without feedback to let staff know when they are doing security correctly or getting it wrong, poor security behaviours can prevail. In addition, some soft punitive measures (e.g. mandatory training courses or briefing sessions for those who aren't adhering to the guidelines or procedures in place) can be effective. These 'deterrents' are fundamental to awareness and part of a multi-layered approach to behaviour change.

5. EVALUATION

As the manager of a campaign, you will need to know if it is working, so that you can build upon its successes and improve any future communications.

Before you embark on a campaign, take a baseline reading of levels of understanding of social engineering and reporting. You can then decide what you want to achieve and how you will measure progress.

The sorts of things that you can baseline and measure over time are:

- Attitudes towards security, including awareness of threat and risk of social engineering
- Current security behaviour
  - Vigilance levels
  - Propensity to report
  - Personal security practice: when online and elsewhere
- Awareness of security campaigns and communications
- Message take-home from such campaigns and communications
- Expected future behaviour
  - Likelihood to report
  - Greater alertness to suspicious behaviour
  - Personal security practice: when online and elsewhere

HOW TO USE THE SOCIAL ENGINEERING CAMPAIGN

B) CREATE A PROJECT PLAN

Next, develop a clear and detailed project plan to enable you to record and track how you intend to manage the running of the campaign.

You should think about:

Creation of a project team, including a project manager

Clarification of the aims of the campaign

When the campaign will have the most impact

The time of year

When to deliver each element of the campaign

Whether all the elements of the campaign are relevant to all staff

What other campaigns might be running, and whether this campaign could potentially conflict with or indeed support them

What other messaging is being given to staff (particularly in relation to social media use and the use of digital devices for work)

Other demands from within the organisation

How to measure the campaign's impact

When to refresh the campaign

Whether you can embed the campaign into long-standing packages such as inductions or security training

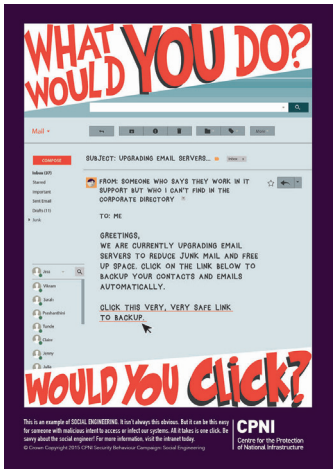
The following matrix is an example of how you can map the five 'Es' to a range of delivery mechanisms. It is not meant to be exhaustive, but provides a range of suggested options that an organisation could use.

EXAMPLE DELIVERY MECHANISM	EDUCATION	ENDORSEMENT	EASE	ENFORCEMENT	EVALUATION
CEO NEWSLETTER	Outline the threat from social engineering and how staff behaviour can aid their own and the organisation's security	Demonstrate that staff have a vital role to play in deterring social engineering	Express where to find details on what social engineering looks like, what an approach looks like and how to report concerns	Express gratitude and thanks to staff for reporting concerns and being vigilant towards the social engineering threat	
SECURITY EVENT	Raise social engineering awareness, give protective security measures and offer suggestions and tips	Have security staff endorse the campaign; convey to staff they have a key role to play in assisting with the organisation's security			
SECURITY MANAGER BLOG	Give examples of social engineering either in the workplace, online or elsewhere and explain the impact; advise on what to look for and how to respond	Convey to employees that security welcome any reports of suspicious activity and will treat every report with due respect	Encourage staff to speak to a member of the security department or call an emergency number	Consider running some tests to evaluate whether the message is reaching staff (e.g. phishing attack experiments or unofficial visitors trying to gain entry to the site). Then let staff know these will be taking place and that security will be having a polite word with all those who are not seen to be following procedure or who aren't being vigilant to the threat.	
POSTERS	Show what social engineering may look like and what to look out for				
GUIDANCE	Provide advice on the threat of social engineering, how to spot it and what to do if you think it is happening to you				
REPORTS INTO SECURITY					Quality and quantity of suspicious activity reports to the security department
STAFF SURVEY					Short interviews with staff to see if they've understood the key messages, how they felt about the campaign and if they've changed their behaviours as a result

ANNEX: MATERIALS IN THIS PACK

Listed below are the various materials included within the CPNI Social Engineering kit that you can use to help deliver your security campaign:

Posters



Video

Guidance, Flier and Checklist

BE SAVVY ABOUT THE SOCIAL ENGINEER:

YOUR GUIDE TO WHAT SOCIAL ENGINEERING IS AND HOW TO PROTECT YOURSELF

CPNI
Centre for the Protection of National Infrastructure