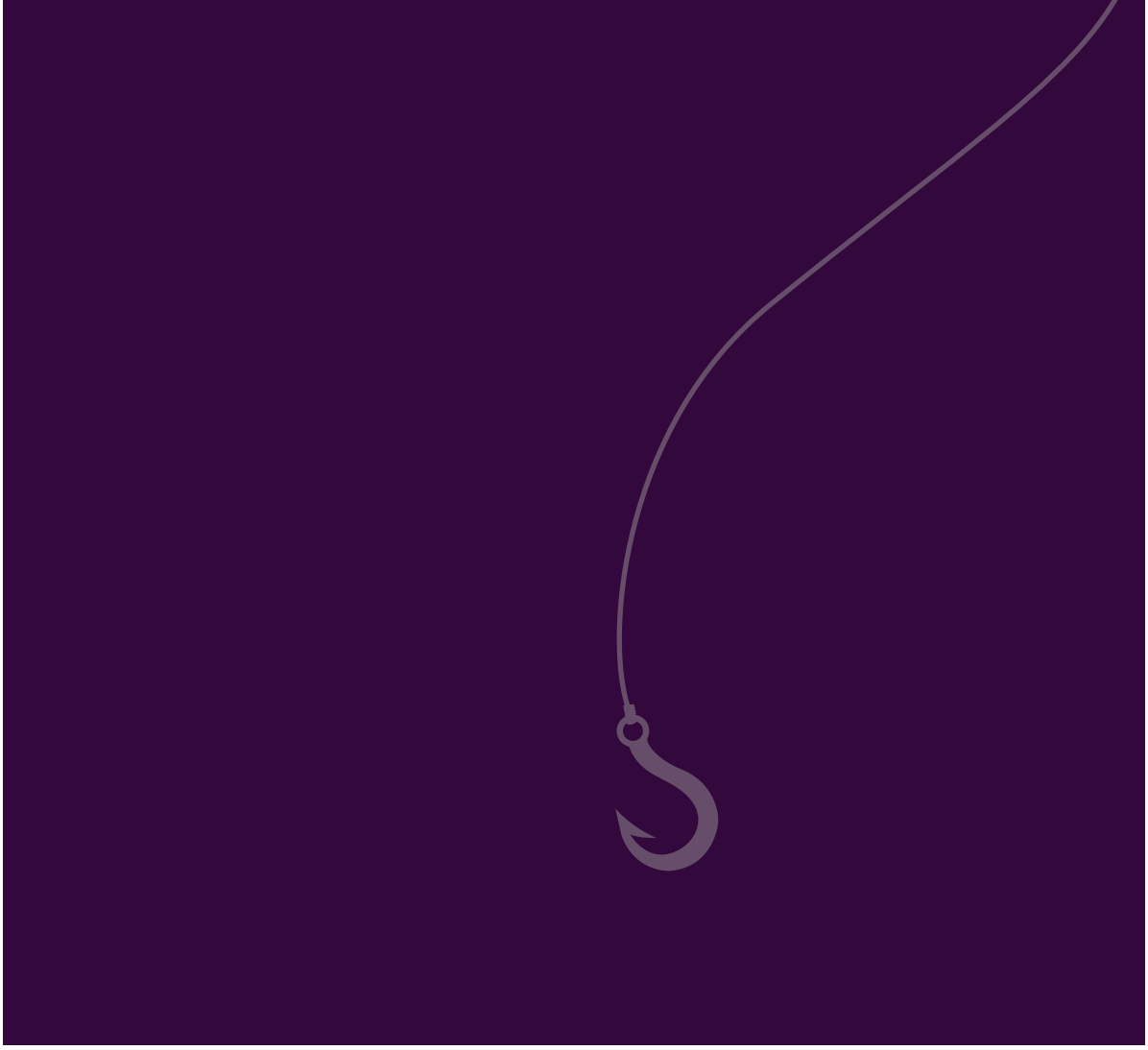
DON'T TAKE THE BAIT

GUIDE FOR ORGANISATIONS:

A personnel security approach to tackling spear phishing

National Protective Security Authority



DISCLAIMER

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favour by NPSA. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, NPSA accepts no liability for any loss or damage (whether direct, indirect or consequential, and including but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using the information contained in this document or its references. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

Organisations face a significant threat from spear phishing. An attack can result in theft of money, intellectual property or sensitive information; loss of revenue, productivity or share price; and damage to reputation. In 2015, the average cost of a spear phishing attack to a UK or US organisation with 1000 employees was $1.6 million[1].

Such attacks are becoming increasingly common and more sophisticated. Because attacks can be cleverly tailored, traditional IT network defences alone are often not enough to detect and prevent them. You can reduce the vulnerability of your organisation by working with employees to dispel the perception that, 'if it gets through the firewall, it is probably genuine'. Your employees have an important role to play in protecting your organisation as a second line of defence, after technical measures.

NPSA's 'Don't Take the Bait' campaign is based on the principle that if you can increase awareness of the scam techniques that are often deployed, then employees will be less likely to fall for them. The theme of the campaign encourages the idea that employees have a role to play in keeping the organisation secure by not falling for, or being tricked by, spear phishing. An important aim of this campaign is for employees to feel encouraged and supported in reporting suspected spear phishing attempts to their organisation - even if this is after they have clicked.

DON'T TAKE THE BAIT!

What is it?

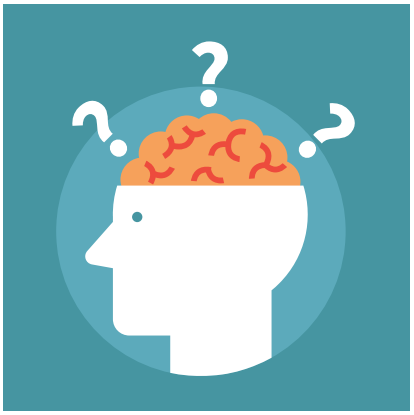
Spear phishing is a targeted type of social engineering attack. An attacker gleans information about an individual which allows them to masquerade as a trusted source in an electronic communication.

This may lead the individual to click on links, accept software updates or open attachments via email, social media messages or electronic pop-up messages.

In doing so, the individual can unwittingly compromise sensitive information, provide access to organisational finances or facilitate technical attacks on company networks.

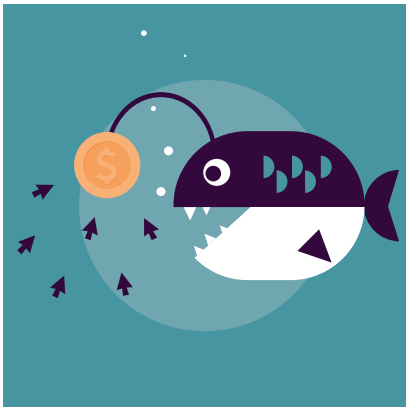
1 Vanson Bourne Spear Phishing Study 2015 https://blog.cloudmark.com/wp-content/uploads/2016/01/cloudmark_survey_infographic.png [Accessed 29 March 2017]

THIS CAMPAIGN ENCOURAGES BEHAVIOUR CHANGE IN THREE MAIN AREAS:



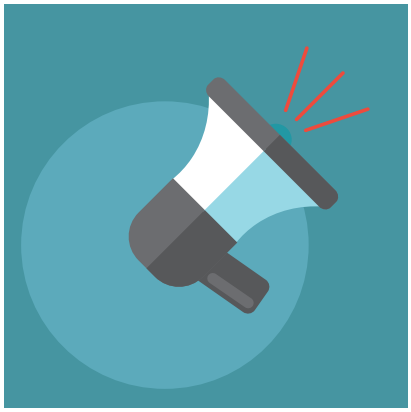
Think before you click

Employees should take the time to pause before responding instead of relying on automatic, habitual clicking behaviour.



Knowing the influence techniques

Employees are able to identify the influence techniques commonly used by spear phishers.



Reporting

Employees report to the organisation when they have seen something suspicious, or where they have clicked and later believe it to be suspicious.

This campaign is designed to motivate employees to play a part in mitigating the threat by improving their capability to spot phishing attempts.

Employees should not be the sole focus of an organisation's protective security efforts to reduce vulnerability to spear phishing. There are a range of useful approaches that can be taken at the organisational level.

TOP TIPS:

• Work on your security culture

This will provide a firm foundation to address phishing with employees. Your campaign will have a much better impact with an actively engaged workforce.

• Encourage reporting

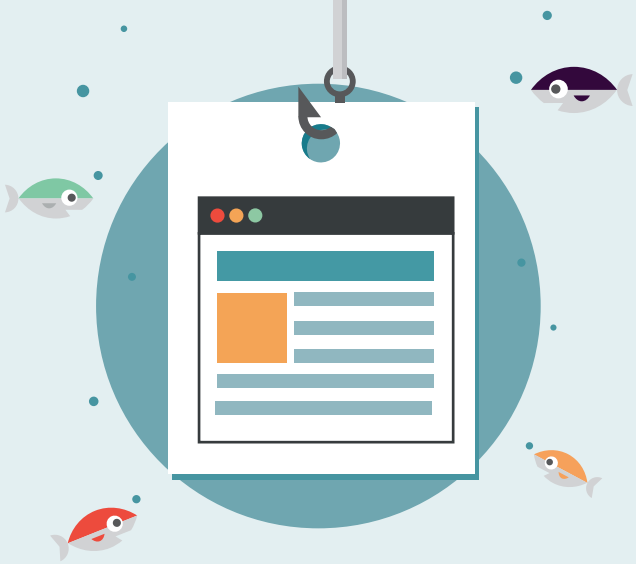
Spear phishing attempts can be difficult to spot. Therefore it is important that you encourage a supportive environment for employees to come forward if they feel they may have responded to something that they now regard as suspicious.

• Encourage digital footprint management

Spear phishers often harvest details of employees from their online profiles and use them to make their approaches more convincing and persuasive. NPSA's digital footprint campaign can help to educate employees (https://www.npsa.gov.uk/security-campaigns/my-digital-footprint).

• Technical defences

Invest in appropriate technical and network controls to limit the amount of potentially malicious emails that employees could face to receive.



• Avoid using a predictable structure for email addresses

(e.g. firstname.surname@organisation.com) These can be easily guessed by an individual looking to target an employee they have found online.

• Phishing simulations

We have produced a handy guide for designing a phishing simulation based on the key questions you would like to answer.

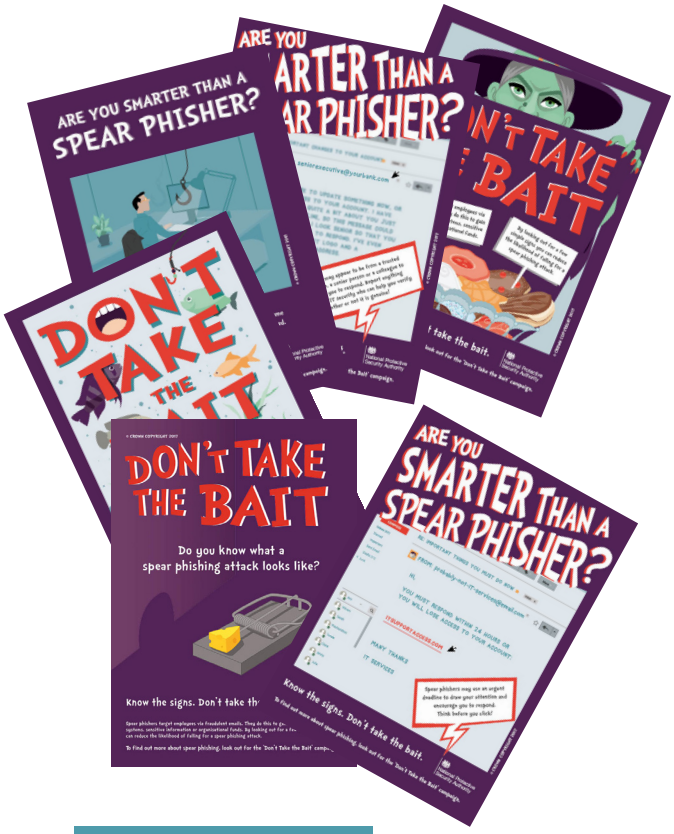
‘DON’T TAKE THE BAIT’ CAMPAIGN MATERIALS

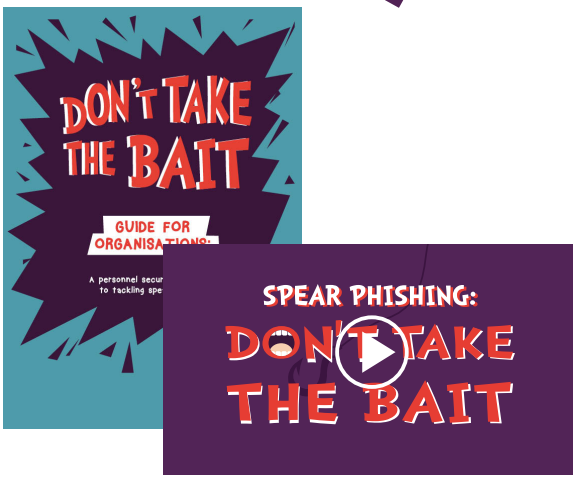
NPSA has developed these materials to help UK organisations to deliver a campaign in-house. A detailed and co-ordinated strategy is required to maximise the impact of your campaign on employee behaviour. This is likely to encompass a campaign project plan, an employee communications plan and the development of additional supporting materials (e.g. intranet articles from a credible source).

NPSA’s ‘Embedding Security Behaviours – Using the 5Es’ guidance is designed to support organisations in improving employee security behaviour (https://www.npsa.gov.uk/embedding-security-behaviour-change).

Don’t Take the Bait campaign materials:

- 1 x animation for employees, to educate on what to look out for with spear phishing
- 1 x infographic for employees, to educate on what to look out for with spear phishing
- 1 x quiz to test employee knowledge levels
- 6 x posters to advertise that your organisation is running the campaign or to demonstrate different forms of spear phishing
- 1 x guide to help organisations develop their own phishing simulation exercises





These materials are available to download on the NPSA website.

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 NPSA logo (e.g. the posters, infographic and quiz). To request access to these editable files, please email NPSA at NPSA-enquiries@npsa.gov.uk.