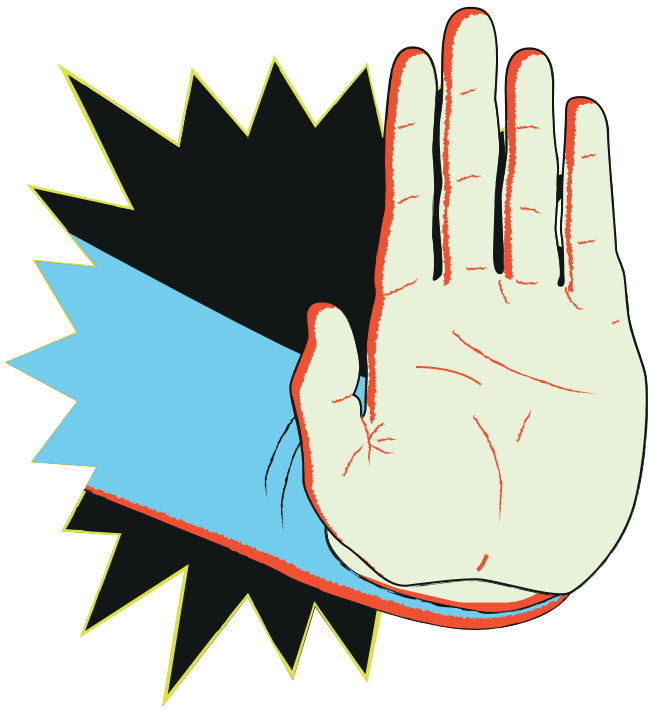
MAIL SCREENING AND SECURITY

A guide for organisations in implementing CPNI's postal security campaign

CPNI
Centre for the Protection of National Infrastructure

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 CPNI. 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, CPNI 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 to the use of this document and seek independent professional advice on your particular circumstances.



MAIL SCREENING MATTERS

This may be an age of increasingly advanced technology, but most organisations still need to use postal and courier services to send and receive physical mail. As a result, there is a risk of receiving something dangerous through the post. Mail streams provide an opportunity for malicious attacks and other security incidents, and this can affect an organisation's day-to-day operations, as well as its reputation.

It's important that your employees understand how to minimise the risk and impact of suspicious mail.

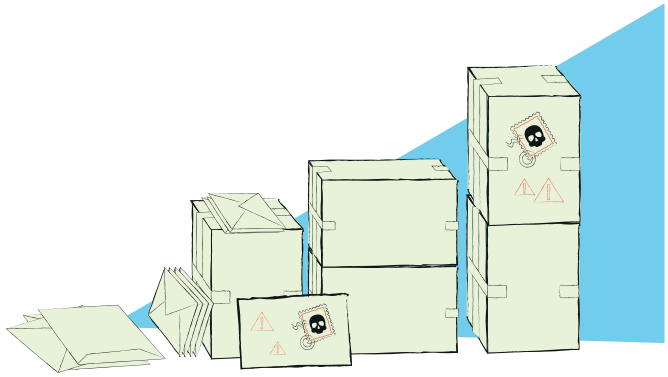
The purpose of CPNI's mail screening and security campaign is to increase awareness around postal security and motivate employees to play their part in mitigating the risk of postal threats. The campaign aims to complement existing guidance within PAS 97 - Mail screening and security - Specification.

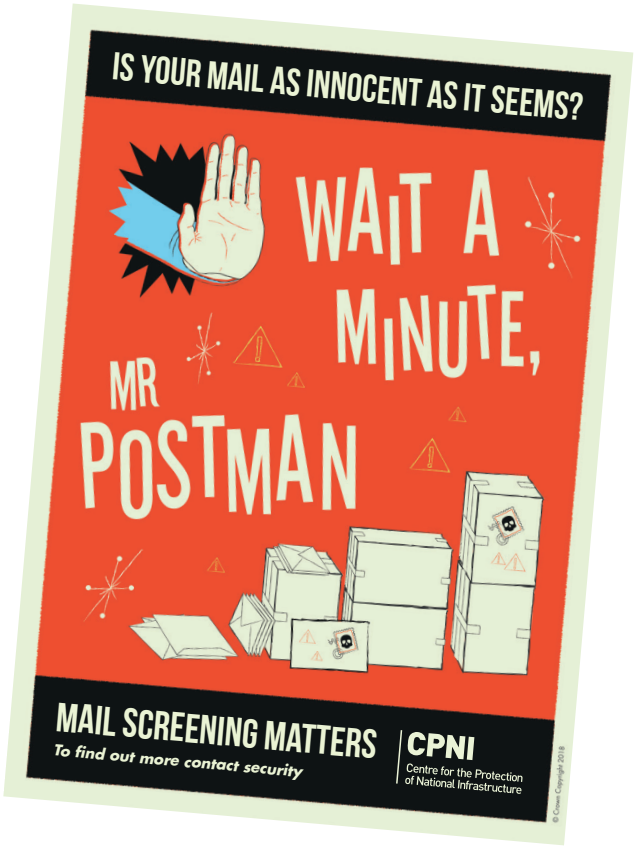
There are several factors to be considered with postal security. This campaign highlights the key parts of the process, such as assessing the risks, developing processes and procedures, and implementing mail security measures. This is communicated through the campaign's variety of resources.

DELIVERING THE CAMPAIGN

CPNI has developed a kit of engaging resources to make it easy to raise awareness through a simple and straightforward campaign. These materials can support current internal procedures and should be used as part of a detailed and co-ordinated strategy, such as an action plan with a timeline, to help maximise its impact and effectiveness.

The resources within this campaign are aimed at three audiences, as described below.





All staff

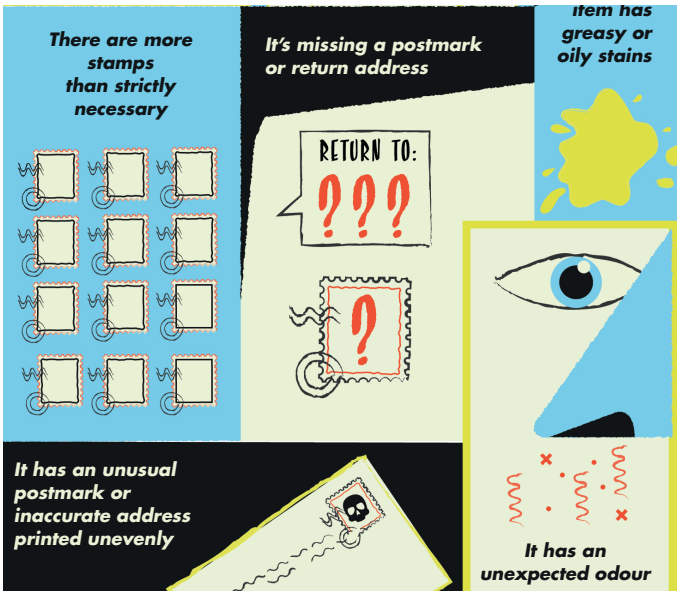
The following materials aim to raise awareness of the importance and relevance of mail security and encourage staff to learn more about their own organisation's procedures.

Materials include:

- A general awareness poster highlighting the campaign to employees, many of whom may not necessarily be in direct contact with mail. It can be used in various locations within an organisation, where appropriate.
- A screensaver for desktop backgrounds or office TV screens.
- Educational case study articles assessing why mail screening matters. These can be put on intranets, used in e-newsletters, or sent out via other means of internal communications. A suggested layout is also included.

Frontline security staff and mail handlers

Employees who handle mail, and security staff with a knowledge of postal security, can use these accessible tools for recognising and responding to a suspicious postal incident.



Materials include:

A poster presenting a summary of potential suspicious indicators, recommended for use in mailrooms and any other locations where mail is received, for example reception areas.

A poster that outlines how to respond to suspicious mail. It should be used together with the 'summary of suspicious indicators' poster to maximise impact, and displayed in mailrooms and any other locations where mail is received.

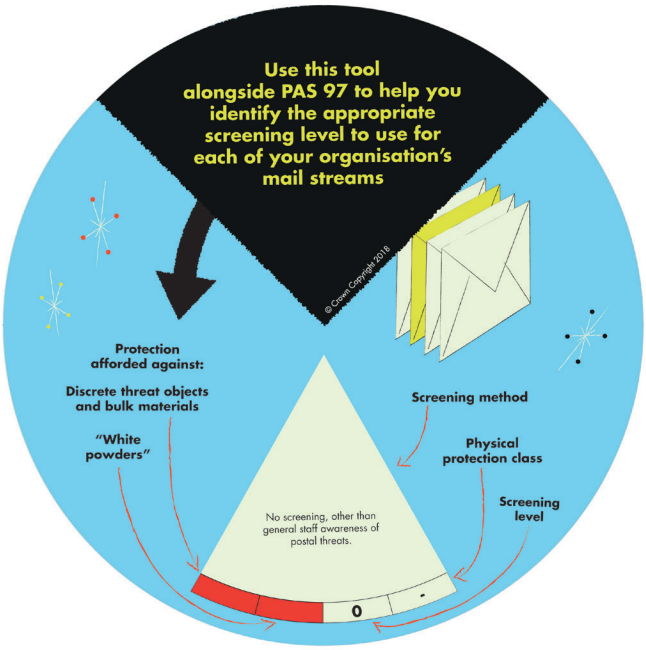
Two factsheets containing a more comprehensive description of potential suspicious indicators, and a detailed version of the recommended response guidance. Available as printouts or digital downloads, these can be used in mailrooms as quick reference guides.

Security managers

The following tools aim to assist those responsible for designing and delivering mail screening procedures in following the guidance contained within PAS 97.

Materials include:

- An editable launch email template that can be personalised and sent out to teams or business groups to introduce the campaign.
- Two editable PowerPoint presentation, one to brief non-mail handling staff on mail screening and security, and a second providing an overview of indicators and response actions for mail handling staff.
- Two factsheets and a PowerPoint presentation summarising the PAS 97 process.
- A tool to help you identify the appropriate screening level for each mailstream within your organisation. This is available in a physical and digital format.



CPNI
Centre for the Protection of National Infrastructure

Every day, our organisation receives and sends mail.

Would you know what to do if one item seemed suspicious?

Introducing CPNI's new mail screening and security campaign

This may be an age of increasingly advanced technology, but our organisation still needs to use postal and courier services to send and receive physical mail. As a result, there is a risk of receiving something dangerous through the post. Mail streams into and within our site present opportunities for malicious attacks or hoaxes, and without the appropriate security measures, security incidents such as these can affect our day-to-day operations, as well as our reputation.

That's why we're taking action with a new mail screening and security campaign.

Over the next few weeks, you'll notice a series of posters, tools, articles and other resources to help you:

- Learn the importance of mail security
- Become aware of our security and mail screening procedures
- Recognise how respond to suspicious mail

If you understand how to minimise the risk and impact of suspicious mail, you can feel equipped in an unexpected situation, and this can safeguard our organisation from a postal threat.

For more information, contact [security personnel] or search for mail screening and security at www.cpni.gov.uk.

https://www.cpni.gov.uk/

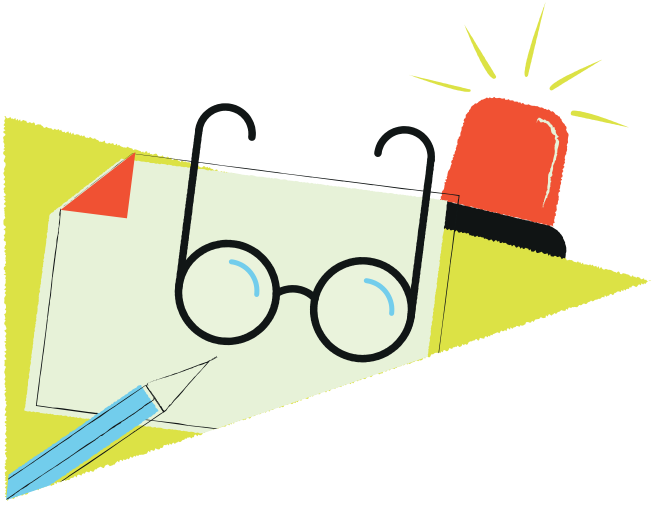
You can update your preferences or unsubscribe from this list.

These materials are all available to download on the CPNI website. Many of the materials in the campaign kit are editable (using InDesign) to allow you to add your own organisation's logo in place of the CPNI logo and include the most suitable contact details.

EXTRA TIPS

Embed a strong security culture

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

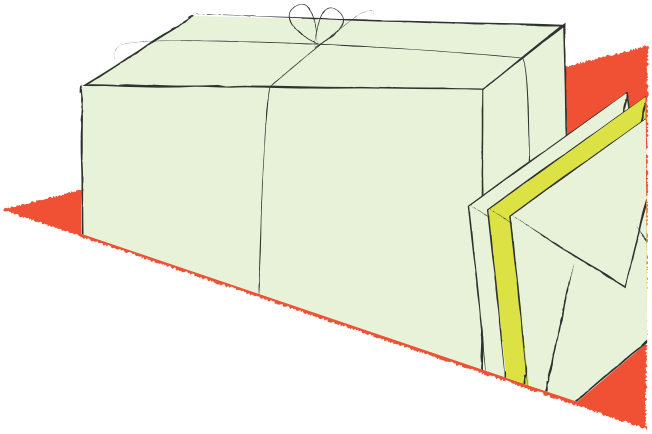


Encourage reporting

Suspicious mail can be difficult to spot. Therefore, it is important you encourage a supportive environment for employees to come forward if they've noticed something unusual.

Make mailrooms your first line of defence

Mailrooms can be used for more than sorting mail and deliveries - they can also provide extra security. A basic level of protection can be achieved by informing mailroom staff to look out for suspicious items, or briefly inspect them, and campaign materials should be clearly placed in these rooms to offer guidance.



To assist your delivery of the campaign, you may want to review CPNI's 'Embedding Security Behaviours: using the 5Es'. This guidance is designed to support organisations in improving employee security behaviour (www.cpni.gov.uk/embedding-security-behaviour-change).

Search for more information on mail screening and security at www.cpni.gov.uk