



POLICE
SCOTLAND
Keeping people safe

Security Advice Document

1. Threat levels

You can check the current threat levels:

- [in the terrorism and national emergencies](#) area on GOV.UK
- [on the MI5 website](#)

The most significant terrorist threat comes from international terrorism. As a number of recent European attacks have showed, attacks may be mounted without warning.

Northern Ireland-related terrorism continues to pose a threat. Dissident republican terrorist groups (such as the Real IRA and the Continuity IRA) have rejected the 1998 Good Friday Agreement. They still aspire to mount attacks within the UK mainland and have conducted attacks within Northern Ireland.

2. STAY SAFE : Terrorist firearms and weapons attacks

Firearms and Weapons attacks are rare in the UK. The 'STAY SAFE' principles tell you some simple actions to consider at an incident and the information that armed officers may need in the event of a weapons or firearm attack:

2.1 RUN

- Escape if you can
- Consider the safest options
- Is there a safe route? RUN if not HIDE
- Can you get there without exposing yourself to greater danger?
- Insist others leave with you
- Leave belongings behind

2.2 HIDE

- If you cannot RUN, HIDE
- Find cover from gunfire
- If you can see the attacker, they may be able to see you
- Cover from view does not mean you are safe, bullets go through glass, brick, wood and metal
- Find cover from gunfire e.g. substantial brickwork / heavy reinforced walls
- Be aware of your exits
- Try not to get trapped
- Be quiet, silence your phone and turn off vibrate
- Lock / barricade yourself in
- Move away from the door

2.3 TELL

Call 999 - What do the police need to know? If you cannot speak or make a noise listen to the instructions given to you by the call taker

- Location - Where are the suspects?
- Direction - Where did you last see the suspects?
- Descriptions – Describe the attacker, numbers, features, clothing, weapons etc.
- Further information – Casualties, type of injury, building information, entrances, exits, hostages etc.
- Stop other people entering the building if it is safe to do so

ARMED POLICE RESPONSE

- Follow officers instructions
- Remain calm
- Can you move to a safer area?
- Avoid sudden movements that may be considered a threat
- Keep your hands in view

OFFICERS MAY

- Point guns at you
- Treat you firmly
- Question you
- Be unable to distinguish you from the attacker
- Officers will evacuate you when it is safe to do so

You must STAY SAFE

- What are your plans if there were an incident?
- What are the local plans? e.g. personal emergency evacuation plan

Further advice

[citizenAID](#) is a simple, clear teaching aid for immediate actions and first aid for a stabbing, bomb incident or mass shooting. Building on Run, Hide Tell, this helps people understand what to do in the event of an attack.

3. Suspicious items - Guidance for the public

- Do not touch
- Try and identify an owner in the immediate area
- If you still think it's suspicious, don't feel embarrassed or think anybody else will report it
- Report it to a member of staff, security, or if they are not available dial 999 (do not use your mobile phone in the immediate vicinity)

- Move away to a safe distance - Even for a small item such as a briefcase move at least 100m away from the item starting from the centre and moving out

Remember - If you think it's suspicious, SAY SOMETHING

4. Suspicious items - Guidance for staff

When dealing with suspicious items apply the 4 C's protocol:-

4.1 CONFIRM whether or not the item exhibits recognisably suspicious characteristics

The HOT protocol may be used to inform your judgement:-

Is it HIDDEN?

- Has the item been deliberately concealed or is it obviously hidden from view?

OBVIOUSLY suspicious?

- Does it have wires, circuit boards, batteries, tape, liquids or putty-like substances visible?
- Do you think the item poses an immediate threat to life?

TYPICAL Is the item typical of what you would expect to find in this location?

- Most lost property is found in locations where people congregate. Ask if anyone has left the item

If the item is assessed to be unattended rather than suspicious, examine further before applying lost property procedures. However, if H-O-T leads you to believe the item is suspicious, apply the 4Cs

4.2 CLEAR the immediate area

- Do not touch it
- Take charge and move people away to a safe distance. Even for a small item such as a briefcase move at least 100m away from the item starting from the centre and moving out
- Keep yourself and other people out of line of sight of the item. It is a broad rule, but generally if you cannot see the item then you are better protected from it
- Think about what you can hide behind. Pick something substantial and keep away from glass such as windows and skylights
- Cordon off the area

4.3 COMMUNICATE - Call 999

- Inform your control room and/or supervisor
- Do not use radios within 15 metres

4.4 CONTROL access to the cordoned area

- Members of the public should not be able to approach the area until it is deemed safe
- Try and keep eyewitnesses on hand so they can tell police what they saw

5. Mail handling

5.1 Small deliveries by courier and mail handling

Most businesses will receive a large amount of mail and other deliveries which offers a potentially attractive route into premises for terrorists. A properly conducted risk assessment should give you a good idea of the likely threat to your organisation and indicate precautions you need to take.

Delivered items which includes letters, parcels, packages, and anything delivered by post or courier, have been a commonly used tactic by criminals and terrorists. Delivered items may be explosive, incendiary, contain sharps, blades or chemical, biological or radiological (CBR) material. The phrase 'white powders' is often used in the context of mail and encompasses CBR material as well as benign materials. Be aware that such materials may not be white and may not be powders.

Anyone receiving a suspicious delivery is unlikely to know which type it is, so procedures should cater for every eventuality. Threat items come in a variety of shapes and sizes; a well-made device will look innocuous, but there may be tell-tale signs.

5.2 Indicators for suspicious deliveries/mail

General indicators that a delivered item may be of concern include:

- unexpected item, especially if hand delivered
- a padded envelope (Jiffy Bag) or other bulky package
- additional inner envelope or other contents that may be difficult to remove
- labelling or excessive sealing that encourages opening at a particular end or in a particular way
- oddly shaped or lopsided
- envelope flap stuck down completely (normally gummed envelope flaps leave slight gaps at edges)
- marked 'To be opened only by...' 'Personal' or 'Confidential'

- item addressed to the organisation or a title (rather than a specific individual)
- unexpected or unusual origin (postmark and/or return address)
- no return address or return address that cannot be verified
- poorly or inaccurately addressed address printed unevenly or unusually
- unfamiliar writing or unusual style
- unusual postmark or no postmark
- more stamps than needed for size or weight of package
- greasy or oily stains emanating from the package
- odours emanating from the package

5.3 Explosive or incendiary indicators

A delivered item may have received some rough handling in the post and so is unlikely to detonate through being moved. Any attempt at opening it, may set it off or release the contents. Additional explosive or incendiary indicators include:

- unusually heavy or uneven weight distribution
- small hole(s) in the envelope or wrapping

5.4 CBR indicators

Additional CBR indicators include:

- powders, liquids emanating from the package
- wrapping stained by liquid leakage
- unexpected items or materials found in the package on opening or x-raying (loose or in a container) such as powdered, crystalline or granular solids; liquids; sticky substances or residues
- unexpected odours observed on opening
- sudden onset of illness or irritation of skin, eyes and nose

5.5 What you can do

Though the precise nature of the incident may not be immediately apparent the first step will be recognition that an incident has occurred, such as through the indicators described above. The response procedure will follow including communication with the emergency services, who will provide the appropriate response. Ensuring that the appropriate staff are familiar with your response procedure is key to its successful implementation.

Some points to consider when planning your response procedure include:

- ensure that forethought is put into communication with both staff and the emergency services
- check that doors can be closed quickly if required
- pre-plan your evacuation routes, ensuring they do not lead building occupants through affected areas. Consider how you will communicate the evacuation routes to occupants during an incident. The level of

evacuation may vary depending on the nature of an incident and may not require the evacuation of your entire building or site

- consult with your Building Services Manager on the feasibility of emergency shutdown or isolation of heating, ventilation and air conditioning (HVAC) systems (including local extraction systems in areas like kitchens) and ensure that any such plans are well rehearsed. Due to the complexity of HVAC systems and the variability across buildings and sites, it is not possible to provide generic advice on the alteration or otherwise of HVAC systems in response to an incident - consultation with your organisation's building services manager and/or specialist HVAC engineers is essential

You don't need to make any special arrangements for medical care beyond normal first aid provision, as emergency services will take responsibility for casualty treatment. However the provision of materials to undertake improvised decontamination, such as absorbent materials and water, in a suitable location, such as where you would likely evacuate contaminated staff to, may be appropriate.

5.6 Actions upon discovery of any suspicious delivered item:

You could discover a suspicious item in a mail room, or anywhere else in the building - ensure you have appropriate emergency response plans in place.

Avoid unnecessary handling and x-raying:

- if you are holding the item, put it down on a cleared flat surface
- keep it separate so it is easily identifiable
- do not move it, even to x-ray it
- if it is in an x-ray facility, leave it there

Move away immediately

- clear immediate area and each adjacent room, including rooms above and below
- if there is any suggestion of chemical, biological or radiological materials, move those directly affected to a safe location close to the incident - keep these individuals separate from those not involved
- prevent others approaching or accessing the cleared areas
- Do not use mobile phones or two-way radios in the cleared area or within fifteen metres of the suspect package.
- Communicate regularly with staff, visitors and the public

Notify police

- if the item has been opened, or partially opened prior to being deemed suspicious, it is vital that this is communicated to the police
- ensure informants and witnesses remain available to brief the police, and that the accuracy of their observations is preserved: encourage witnesses immediately to record their observations in writing, and

discourage them from discussing the incident or their observations with others prior to the arrival of the police

If a CBR incident is suspected

- undertake improvised decontamination of contaminated people as quickly as possible, ideally within the first 15 minutes
- Do not use lifts to move around, or evacuate the building
- If the alteration of the HVAC system features within your response plan, this should be undertaken as quickly as possible

- If in doubt call 999 and ask for the police
- Clear the area immediately
- Do not attempt to open the letter or package
- Avoid unnecessary handling
- Keep it separate so it is easily identifiable.

[Further advice on screening mail and courier deliveries](#)

6. Bomb threat guidance

The vast majority of bomb threats are hoaxes designed to cause alarm and disruption. As well as the rare instances of valid bomb threats, terrorists may also make hoax bomb threat calls to intimidate the public, businesses and communities, to draw attention to their cause and to mislead police. While many bomb threats involve a person-to-person phone call, an increasing number are sent electronically using email or social media applications.

No matter how ridiculous or implausible the threat may seem, all such communications are a crime and should be reported to the police by dialling 999

It is important that potential recipients - either victims or third-parties used to pass the message - have plans that include how the information is recorded, acted upon and passed to police.

6.1 The bomb threat message

Bomb threats containing accurate and precise information, and received well in advance of an actual attack, are rare occurrences. Precise motives for hoaxing are difficult to determine but may include revenge, extortion, a desire to impress, or a combination of these and other less understandable motives. The vast majority of cases are hoaxes and the intent is social engineering, to cause disruption, fear and/or inconvenience the victim.

6.2 Communication of the threat

A bomb threat can be communicated in a number of different ways. The threat is likely to be made in person over the telephone; however, it may also be a

recorded message, communicated in written form, delivered face-to-face or, increasingly, sent by email or social media (e.g. Twitter or Instagram, etc.). A threat may be communicated via a third-party, i.e. a person or organisation unrelated to the intended victim and identified only to pass the message.

6.3 Immediate steps if you receive a bomb threat communication

Any member of staff with a direct telephone line, mobile phone, computer or tablet etc., could conceivably receive a bomb threat. Such staff should, therefore, understand the actions required of them as the potential first response to a threat message.

If you receive a telephone threat you should:

- stay calm and listen carefully
- have immediate access to a checklist on key information that should be recorded (see bomb threat checklist - attached)
- if practical, keep the caller talking and alert a colleague to dial 999
- if displayed on your phone, note the number of the caller, otherwise, dial 1471 to obtain the number once the call has ended
- if the threat is a recorded message write down as much detail as possible
- If the threat is received via text message do not reply to, forward or delete the message. Note the number of the sender and follow police advice
- know who to contact in your organisation upon receipt of the threat, e.g. building security/senior manager. They will need to make an assessment of the threat

If the threat is delivered face-to-face:

- try to remember as many distinguishing characteristics of the threat-maker as possible

If discovered in a written note, letter or as graffiti:

- treat as police evidence and stop other people touching the item

If the threat is received via email or social media application:

- do not reply to, forward or delete the message
- note the sender's email address or username/user ID for social media applications
- preserve all web log files for your organisation to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

REMEMBER Dial 999 and follow police advice. Seek advice from the venue security/operations manager as soon as possible

6.4 Assessing the credibility of bomb threats

Evaluating the credibility of a threat is a critical task, particularly if the attack being threatened is imminent. This is a tactic used to place additional pressure on decision makers. Police will assess the threat at the earliest opportunity. When specific intelligence is known to police, advice will be issued accordingly; however, in the absence of detailed information, it will be necessary to consider a number of factors:-

- is the threat part of a series? If so, what has happened elsewhere or previously?
- can the location of the claimed bomb(s) be known with precision? If so, is a bomb visible at the location identified?
- considering the hoaxer's desire to influence behaviour, is there any reason to believe their words?
- if the threat is imprecise, could an external evacuation inadvertently move people closer to the hazard?
- is a suspicious device visible?

6.5 Actions to consider

Responsibility for the initial decision making remains with the management of the location being threatened. Do not delay your decision making process waiting for the arrival of police. Police will assess the credibility of the threat at the earliest opportunity. All bomb threats should be reported to the police and their subsequent advice followed accordingly. It is essential that appropriate plans exist, they should be event and location specific. Venue options to manage the risk include:-

External evacuation

Leaving the venue will be appropriate when directed by police and/or it is reasonable to assume the threat is credible, and when evacuation will move people towards a safer location.

It is important to appoint people, familiar with evacuation points and assembly (rendezvous) points, to act as marshals and assist with this procedure. At least two assembly points should be identified in opposing directions, and at least 500 metres from the suspicious item, incident or location. Where possible the assembly point should not be a car park. You may wish to seek specialist advice, which can help to identify suitable assembly points and alternative options as part of your planning. It is essential that evacuation plans exist; they should be event and location specific. Evacuation procedures should also put adequate steps in place to ensure no one else enters the area once an evacuation has been initiated.

The police will establish cordons depending upon the size of an identified suspect device. Always follow police directions and avoid assembly close to a police cordon.

Internal or inwards evacuation ('invacuation')

There are occasions when it is safer to remain inside. Staying in your venue and moving people away from external windows/walls is relevant when it is known that a bomb is not within or immediately adjacent to your building.

If the suspect device is outside your venue, people may be exposed to greater danger if the evacuation route inadvertently takes them past the device. A safer alternative may be the use of internal protected spaces. This type of inwards evacuation needs significant pre-planning and may benefit from expert advice to help identify an internal safe area within your building. These locations should be in your plans.

If the location of the device threatened is unknown, evacuation represents a credible and justifiable course of action.

Decision not to evacuate or inwardly evacuate

This will be reasonable and proportionate if, after an evaluation by the relevant manager(s), the threat is deemed implausible (e.g. a deliberate hoax). In such circumstances police may provide additional advice and guidance relating to other risk management options. It may be considered desirable to ask staff familiar with the venue to check their immediate surroundings to identify anything out of place, see search considerations below.

Checking your venue for suspicious items - Search considerations

Regular searches of your establishment, proportionate to the risks faced, will enhance a good security culture and reduce the risk of a suspicious item being placed or remaining unnoticed for long periods. Additionally, if you receive a bomb threat and depending upon how credible it is, you may decide to conduct a 'search' for suspicious items. To that end:

- ensure plans are in place to carry out an effective search in response to a bomb threat
- identify who in your venue will coordinate and take responsibility for conducting searches
- initiate a search by messaging over a public address system (coded messages avoid unnecessary disruption and alarm), by text message, personal radio or by telephone cascade
- divide your venue into areas of a manageable size for 1 or 2 searchers. Ideally staff should follow a search plan and search in pairs to ensure nothing is missed
- ensure those conducting searches are familiar with their areas of responsibility. Those who regularly work in an area are best placed to spot unusual or suspicious items
- focus on areas that are open to the public; enclosed areas (e.g. cloakrooms, stairs, corridors, lifts etc.) evacuation routes and assembly points, car parks, other external areas such as goods or loading bays

- develop appropriate techniques for staff to be able to routinely search public areas without alarming any visitors or customers present
- under no circumstances should any suspicious item be touched or moved in any way. Immediately start evacuation and dial 999
- ensure all visitors know who to report a suspicious item to and have the confidence to report suspicious behaviour

Remember: it is vital that regular drills are carried out to ensure all are familiar with bomb threat procedures, routes and rendezvous points. Disabled staff should have personal evacuation plans and be individually briefed on their evacuation procedures. Similarly all visitors should be briefed on evacuation procedures and quickly identified and assisted in the event of a threat.

Familiarising through testing and exercising will increase the likelihood of an effective response to an evacuation and aid the decision making process when not to evacuate/invacuate.

6.6 Media and communication

Avoid revealing details about specific incidents to the media or through social media without prior consultation with police. Do not provide details of the threat, the decision making process relating to evacuation (internal or external) or why a decision not to evacuate was taken.

Releasing details of the circumstances may:

- be an objective of the hoaxer and provide them with a perceived credibility
- cause unnecessary alarm to others
- be used by those planning to target other venues
- elicit copycat incidents
- adversely affect the subsequent police investigation

7. Insider threat

Occasionally threats to companies and organisations come from within. Whether it is from a disaffected member of staff or an employee that has misrepresented themselves, there is more opportunity to disrupt or cause damage (whether physical or reputational) from the inside.

The risks posed by the insider threat can be lessened by carrying out thorough pre-employment checks and by having a strong security culture. The CPNI provides detailed guidance on [personnel security](#).

8. Cyber threat

In the 21st century, one of the greatest threats to a company or organisation is from cyber attacks. The effects can often be devastating: the loss of crucial data, or a reduction in operating efficiency, or even closure.

Your senior management must assess the risk appetite of the company or organisation. But it is vital that everyone in your workplace understands the risks posed by cyber attacks.

A cyber attacker may not reveal themselves or even the nature of the attack. An attack may have no obvious adverse effects, but will extract information or data from your networks.

Read the advice on [Cyber essentials](#) or visit the [CPNI Website](#).

•

9. Further information and advice

For further information follow the links to the [NaCTSO](#) and [CPNI](#) website or the links below.

- More documents and information regarding [managing the risks from terrorism](#)
- For an overview of the protective security measures available, read [‘Protecting against terrorism’](#)
- National Counter Terrorism policing is providing advice to the public on the steps they can take to keep themselves safe in the rare event of a firearms or weapons attack - [RUN HIDE TELL](#)
- [Employee Vigilance Campaign](#) Assists organisations to highlight the importance of reporting all kinds of unusual activity and behaviour
- [Advice on professionalising security](#)
- [Advice on CCTV](#)
- [Advice for disrupting hostile reconnaissance](#)