ProtectUK

Other Threats

ProtectUK publication date
06/10/2022

Does an item look lost or suspicious? If so, you should consider the HOT protocols.
Is it: Hidden? Overly suspicious? Typical?

The HOT protocols and suspicious items

Consider the HOT protocols

Hidden

Has the suspicious item been concealed or hidden from view?

Obviously suspicious

Does it have wires, circuit boards, batteries, tape or putty-like substances? 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
- If after applying the HOT protocols you still believe the item to be suspicious, call 999

Delivered items

Letters, parcels, packages and other items delivered by post or courier have been used on occasions to disguise harmful devices and substances.

Delivered items may be explosive, incendiary, include sharps or blades, or contain chemical, biological or radiological material.

Other hazardous or offensive material such as faeces have also been used in delivered items. Anyone receiving a suspicious delivery is unlikely to know what type it is, so procedures and precautions should cater for every eventuality.

A delivered item will probably have received fairly rough handling in the post, so is unlikely to detonate because it is moved. Any attempt to open such an item may activate it.

Threat items come in a wide range of shapes and sizes. A well-made device will look innocuous but may still have tell-tale signs.

Indicators of a suspicious delivered item

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

- an unexpected item, especially if hand delivered
- a padded envelope (Jiffy Bag) or other bulky package
- an 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
- an envelope flap stuck down completely (normally gummed envelope flaps leave slight gaps at edges)
- marked ‘to be opened only by...’ ‘personal’ or ‘confidential’
- an 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 package
- odours emanating from package

Explosive or incendiary indicators

Additional explosive or incendiary indicators include:

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

White powder (CBR) indicators

Additional chemical, biological or radiological (CBR) indicators include:

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

For more information, refer to our Guidance on hazardous substance exposure page: REMOVE, REMOVE, REMOVE

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

Bomb threats

If you receive a telephone bomb threat, you should:

- stay calm and listen carefully
- note the callers number, otherwise, dial BT 1471 to obtain the number once the call has ended
- record the call if you’re able to do so
- if practical, keep the caller talking and alert a colleague to dial 999
- 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

If the bomb 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 user name/user ID for social media application
- preserve all web log files to help the police investigation

Remember: Dial 999 and follow police advice.

Telephone threats and anonymous calls

Anonymous calls and telephone threats are usually intended to lower your morale or cause fear, alarm and distress.

These calls can be extremely distressing, but if it is bearable, keeping the caller talking can reveal important information.

If possible keep a note pad and pen to hand.

If the call is not too upsetting, consider the following actions:

- write down the details immediately, including date, time, length of call and exact words spoken
- note details about the caller; like gender, accent, a speech impediment
- listen for any clues as to the intention of the caller or the specific threat
- listen for background noise, which may provide valuable information about the location or circumstances of the caller (traffic, trains, children)
- on termination of the call, operate any trace facility, such as BT 1471 service, and write down the number if registered
- inform the police immediately if threats have been made
- tell your children to hang up without responding, if they received such a call. You may decide that your children should not answer the telephone if there is a risk of a malicious call
- if you are persistently receiving silent calls, do not say anything when you answer. Legitimate callers will identify themselves and if it is the malicious caller you can hang up

Preventative action you can take:

- ensure you home phone number is ex-directory
- use a caller display function, so that the call can be screened before being answered
- amend the outgoing message on your answer machine or voicemail. You should not provide

any personal information or indicate that you are away from your property for any length of time
- the use of social media, smartphones and tablets has increased the potential for theft of information that could be used to target you. Get Safe Online provides practical advice on how to protect yourself, your computers, mobile devices and your business against fraud, identity theft, viruses and many other problems encountered online
- consider registering with the Telephone Preference Service (TPS). TPS is the UK's only official 'Do Not Call' register for landline and mobile numbers. It allows individuals and businesses to opt out of unsolicited live sales and marketing calls. It's free to register a telephone number

Mobile devices

You need to be aware of the security risks and take steps to protect your devices. Think about the activities you use your device for, such as online banking, personal emails, social media and photographs. Could these be made public or used against you?

- use all of the security facilities available, like device tracking, screen and SIM passcodes
- disable your Wi-Fi and Bluetooth connection when not in use
- record the IMEI numbers for your phone and tablet. An IMEI is 15 numbers long and uniquely identifies your phone. It can be found on the phone box package, under the phone battery or by typing *#06# into your phone
- change the default PIN for voicemail access
- avoid using public Wi-Fi hotspots. These may not be secure
- disable location services where possible and review privacy settings to prevent someone tracking your movements and identifying your home address or place of work
- geotagging marks a video, photo or other media with a location, this can reveal private information to a third party*
- remove metadata from pictures, especially ones taken from mobile phones before you post them online**

* Geotagging captures the image's location through latitude, longitude, altitude and compass bearing.
** Metadata can be the basic data such as author, date created, date modified and file size. Metadata can be created manually or through automation.

Further information

Read the NPSA's booklet: My Digital Footprint - A brief guide

www.getsafeonline.org

www.tpsonline.org.uk

www.npsa.gov.uk

https://www.protectuk.police.uk/

PAGE CATEGORY

AWARENESS