PROTECT YOURSELF

A guide to personal security

NaCTSO
National Counter Terrorism Security Office

Making common sense common practice

Effective personal security

Protecting yourself and your family

Our own security, and the safety of those close to us, is of utmost importance.
The more you do to protect yourself, the safer you and your family will be.

Personal security means taking personal responsibility

While it is impossible to provide security for every eventuality this guide provides generic advice and identifies other valuable sources of information.

In this guide, we'll give you advice on how to stay safe at home, at work, on-the-move and online.
The recommendations are based on research, but they are ultimately common sense precautions.
By adapting them to your individual needs you can create a firm foundation for your personal security.

Exactly which measures you adopt will depend on the extent or level of threat you are likely to encounter. To help assess this, consider the following:

- Your profession – does the role you perform make you an attractive target?
- Specific threats – is there credible intelligence to suggest you are at risk?
- Your personal history – have you been targeted in the past?

The measures you take should be appropriate to the perceived threat. If they are excessive, they may cause unnecessary inconvenience and stress; if they are insufficient, you may put yourself at risk.

The aim of this booklet is to protect and prepare you so that you and those around you can be assured that all sensible precautions have been taken.

No-one has more responsibility for your personal security than you. Today, individuals face a range of potential threats – from criminals to extremists. Do not make their job easier through complacency.

This guidance book provides some technical detail. Please seek the support of a security professional from the relevant accredited body where required.

Identifying vulnerability

Vulnerability means there is a risk of successful attack

It is important you learn to recognise situations where you are vulnerable, so you can avoid them or – if this is not possible – be on your guard. For example, most people are relatively vulnerable when answering the door at home, preparing to drive off in their car or at any time when their movements can be predicted. Attackers can be creative when it comes to finding ways and means to target individuals and their families. The objective may be to cause embarrassment, inconvenience and distress, but may also include the intent to cause physical injury or threaten life itself.

No one can be on 'high alert' 24 hours a day. The information in this booklet will help you decide where you need to take precautions, when to maintain heightened awareness and when you should involve the police.

Good personal security should take into account both your work and home life. Here are some effective measures you can take .This list is not exhaustive and the precautions you use will depend on your individual circumstances.

Security at home

House and grounds

- To deter intruders, the perimeter of the property should be made as secure as possible. Keep fences and walls in a good state of repair.
- It is important that boundaries clearly define the difference between public and private space. Front boundaries should be kept low, not exceeding 1.0m in height, to remove hiding places and enable good natural surveillance. Side and rear boundaries should provide robust defensive barriers to a minimum height of 1.8m. An additional diamond style trellis topping is difficult to climb and provides an ideal framework for spiky defensive planting, such as climbing roses.
- Side and rear gates should be the same height as the side and rear boundaries (minimum 1.8m), be lockable and located at or as close to the front building line as possible to avoid recessed areas.
- Garages, outbuildings and sheds should be kept locked when not in use.
- Metal up-and-over garage doors can be secured by fitting purpose made locks to either side, approximately 300mm up from the floor or by fitting an external floor mounted, locking 'T' bar with a closed shackle padlock.
- Wooden garage double doors can be secured externally with two substantial hasps and staples with closed shackle padlocks, one towards the top and one towards the bottom to reduce leverage points.
- Wooden side and rear doors can be secured with a BS 3621: 2007 5-lever mortice deadlock or sash lock fitted half way up the leading edge of the door, with internal locking throw bolts or mortice rack bolts fitted one third from the top and bottom to reduce leverage points.
- Shed doors can be secured externally with two substantial hasps and staples with closed shackle padlocks, one towards the top and one towards the bottom to reduce leverage points. External hinge screws should be replaced with security screws to prevent them being removed and access gained this way.
- Windows should have key operated locks and can be further secured with internal diamond mesh grilles.
- Check garage doors and windows each morning for signs of forced entry.
- Ensure tools and ladders, which could be used to access your home, are locked away.
- Keep the area around your home clear and tidy. This will enable you to identify unusual or suspicious objects quickly and remove anything that could potentially be used to cause damage, e.g. loose bricks, large stones and garden ornaments.
- If possible, keep your dustbin/recycling bins behind secure gates until collection day to prevent them being used as climbing aids.

Doors, windows and locks

A large proportion of newly built properties have been awarded Secured by Design (SBD) certification, which means that they have had attack tested doors and windows installed under the SBD Scheme. Some existing properties have had their doors and/or windows replaced with attack tested products that meet BS PAS 24:2012 or the equivalent, which includes the door and/or window, frame, locks, fittings and glazing. If there is documentation to confirm that this is the case, the measures detailed in this section will not be required. Alternatively there may be documentation to prove that an existing building has had the doors and/or windows replaced to the above standard. Further information is available at: www.securedbydesign.com

- Establish a routine for completing checks to confirm all doors and windows are secure before going to bed or leaving the house.
- Ensure good quality locks are fitted to external doors and access windows.
- Solid timber doors should be at least 44mm thick and supported with substantial hinges. Hinge bolts (metal pins that automatically engage or disengage as the door is opened or closed) can provide additional security, particularly for outward opening doors where the hinges are exposed.
- A house with a solid timber front door should have a Kitemarked BS 3621: 2007 5-lever mortice deadlock (single point locking mechanism that can be opened or deadlocked with a key from both the inside and outside), fitted one third of the way up the leading edge.
- A solid timber front door belonging to a flat or house that has been converted into flats or separate rooms should have a Kitemarked BS 8621: 2007 deadlock (all of the security benefits of a BS 3621: 2007 lock, but has an internal thumb turn to enable quick exit without a key), fitted one third of the way up the leading edge of the door (see LACORS Housing - Fire Safety Guidance).
- A surface mounted BS 3621: 2007 automatic deadlocking rim latch lock for a house or BS 8621: 2007 automatic deadlocking escape night latch lock for flats or separate rooms in converted houses should be fitted one third of the way down the leading edge.
- Fit a Door and Hardware Federation Technical Specification (DHF TS) 003 door chain or limiter to outer doors and make sure you use it.
- Fit an internal shield/cowl (letter guard) to prevent car and house keys being fished through the opening. Alternatively, if the risk dictates, either blank off the letterbox slot and fit an external mailbox or fit an internal fire-proof letterbox.
- To protect thumb turn locks from being opened from outside, adjacent glass panels should be replaced with laminated glass which meets the minimum requirements of BS EN 356: 2000 class P1A. Alternatives are LPS 1175 SR1 or STS 202 BR2 fixed internal grilles or security film.
- If the door has a key operated multi-locking mechanism, make sure that you always lock it with a key. Simply closing the door and pushing the handle up will not prevent someone entering. You must push the handle up to engage the multi-locking mechanism and then use the thumb turn or key to lock it – LIFT, LOCK, REMOVE (if you have a key). Remember to keep the key out of sight but in a secure place in case of fire.
- A UPVC, aluminium or composite door, including external double/French or patio doors, will often have a multi-point locking mechanism. This should include either a DHF TS 007 Kitemarked 3-star cylinder or alternatively a DHF TS 007 1-star cylinder plus a pair of DHF TS 007 2-star handles. If not, these can usually be upgraded quickly and easily.
- Solid timber side and rear doors should have a BS 3621: 2007 5-lever mortice deadlock or sash lock fitted half way up the leading edge of the door, with locking throw bolts or mortice rack bolts fitted one third from the top and bottom on the leading edge.
- Lower hardwood panels can be reinforced internally with a 12mm overlapping plywood panel, glued and screwed into the door. The void created between the existing hardwood panel and the overlapping plywood panel should be in filled with chipboard of an appropriate thickness.
- Patio doors should have a minimum of three locking points, with an anti-lift device to prevent the sliding door being lifted off its track. Surface mounted patio locks can be fitted to provide additional security.
- Solid timber external glazed double doorsets should have a Kitemarked BS 3621:2007 5-lever mortice sash lock fitted half way up the leading edge, with either mortice rack bolts or surface mounted locking throw bolts fitted to the top and bottom of each of the two doors, securing into the frame, not into the opposing leaf.
- Double doors require two pairs of hinge bolts located as close as possible to the hinges. Alternatively, new hinges with integral bolts can be fitted.
- A DHF TS 002 door viewer or audio/visual door entry system (video entry/intercom) will enable you to identify callers before you open the door. Even then, only open the door with the chain or limiter on.
- All accessible windows should have key operated locks, unless they are designated fire escape routes. Ideally windows will have multi-point locking, but if not, additional surface mounted key operated locks can be fitted.
- Easily accessible externally beaded windows should have the glazed panels secured with security clips, double sided security tape or silicone sealant which has been applied to the frame and the glazed panel bedded onto it.
- Obscure the view into your home by fitting blinds, curtains or film including glazed exterior doors. Get into the habit of closing curtains or blinds when occupying a well-lit room.
- If you replace doors, windows and security products, ensure they have been tested to withstand attack and meet one of the following standards: For doors: PAS 24:2012, STS 201, STS 202 BR2, LPS 1175 SR2 or LPS 2081 SR B. For windows: PAS 24:2012, STS 204, LPS 1175 SR1 or LPS 2081 SR A.

Further guidance is available at: www.securedbydesign.com

All security improvements should be made in consultation with your insurance company.

Key care

- Do not leave a key under the doormat or in other obvious hiding places. It is better to give responsible members of the household their own keys.
- Do not label your keys – if you need to identify keys, use a colour-code theme.
- Keep control of your door keys, make sure you know who has copies and if you cannot account for all the keys, change the locks. Do not give keys to people you do not know, e.g. trades people.
- Make sure the keys for doors and windows which could be used to exit the building in the event of a fire are readily accessible. They should not be visible or easily reached from outside.

Alarms

Intruders do not want to be seen or heard so setting off an alarm and attracting attention is their enemy. Police recommend that you select an installer who is affiliated to one of the recognised alarm inspectorate bodies, such as the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB).

Generally, there are three types of intruder alarm system:

1. Monitored – which may provide a police response via the alarm company.
2. Speech dialler – which automatically calls pre-programmed key-holders (not police).
3. Audible only – which relies on neighbours and passers-by to react.

- To maximise the deterrent, place external, active alarm bell boxes with flashing lights and sounders at the front and back of the property (burglar alarms).
- Consider fitting mains-operated smoke detectors or a fire alarm system in your home, if there is not already one installed. Have a fire extinguisher for example, available for emergencies.

Be aware that DIY alarms will not necessarily receive a police response.

Lighting

- Good external lighting can help to deter intruders.
- Low wattage lighting is recommended to illuminate all external doors, car parking and garage areas and footpaths leading to your home.
- External lighting should switch on using a photo electric cell (dusk to dawn) with a manual override.
- Bollard lighting is not recommended as it does not project sufficient light at the right height to aid facial verification and reduce the fear of crime.
- Consider fitting other forms of security lighting for use in emergencies or if suspicion is aroused. Floodlights, sited in strategic places, make it difficult for would-be assailants to hide from view.
- Always have reserve lighting available such as a torch.

CCTV

- (From 2016) If your domestic CCTV system covers any areas beyond your boundaries, even partially, then it will be subject to the Data Protection Act and must be registered with the Information Commissioner's Office (ICO). For more information about the legal requirements of CCTV, please visit the ICO's website at: ico.org.uk/for-the-public/cctv
- Seek further advice from a professional CCTV installer accredited to one of the recognised CCTV inspectorate bodies, such as the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB).

Visitors

- Positively identify callers before opening the door.
- Ask friends and relatives to inform you of intended visits.
- Arrange fixed times for tradespeople to call; check their identity on arrival and never leave them alone in the house.
- Be wary of late night callers to your home.
- Instruct children never to answer the door or let strangers in to your home. Tell them to fetch an adult to do it.

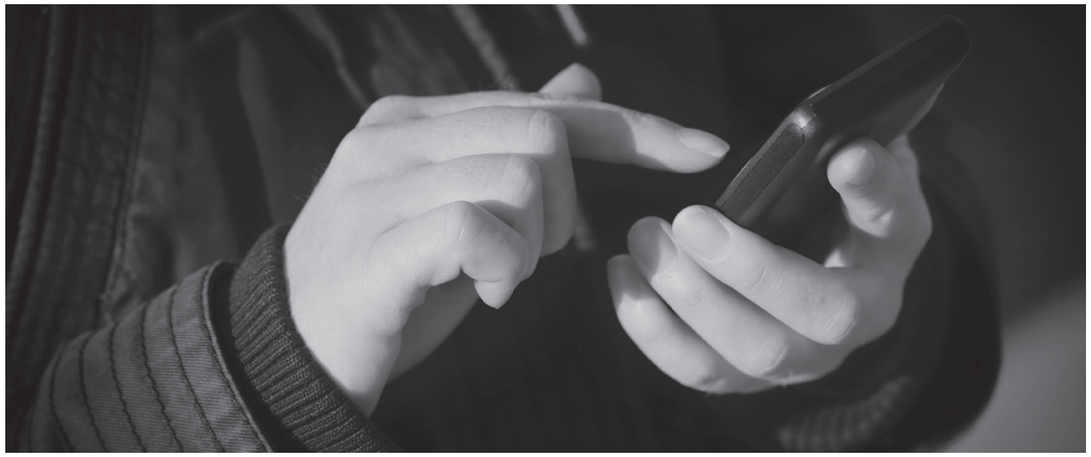
Confidential waste

When discarding sensitive, confidential or personal material, ensure that you treat it as confidential waste:

- Do not place it directly in the bin, separate it from normal waste.
- Shred it, put it in a confidential waste bag and keep it safe, not in a public area, until it can be disposed of correctly.
- Carefully dispose of CDs, DVDs, USBs, PCs, laptops, tablets and other devices that contain sensitive, confidential or personal data.
- There are reputable companies that specialise in confidential waste disposal.

Firearms and weapons attack

'Stay Safe' principles (Run Hide Tell) give some simple actions to consider at an incident and the information that armed officers may need in the event of a firearms and weapons attack. Full guidance is contained on the NaCTSO website **www.gov.uk/government/publications/recognising-the-terrorist-threat**



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.

Hide

- If you can't 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 / reinforced walls.
- Be aware of your exits.
- Try not to get trapped.
- Be quiet, silence your phone.
- Lock / barricade yourself in.
- Move away from the door.

Tell

Call 999 – What do the police need to know?

- 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.

Street safety

Suzy Lamplugh Trust highlight that it takes three things for a violent or aggressive incident to happen – a victim, a perpetrator and an opportunity. By taking some suitable safety precautions, you can reduce the opportunities and therefore the risk of experiencing violence or aggression.

- Plan ahead, before you go out think about how you are going to get home. Can you travel home with a friend? What time does the last bus/train leave?
- Avoid danger points like quiet or poorly lit alleyways, subways or isolated car parks. Walk down the middle of the pavement if the street is deserted.
- If you do have to pass danger points, think about what you would do if you felt threatened.
- Consider heading for a public place; somewhere you know there will be other people, for example a garage or shop.
- If you are at all worried, try and stay near a group of people.
- Try to keep both hands free and do not walk with your hands in your pockets.
- Try to use well-lit, busy streets and use the route you know best.
- Whenever possible, walk facing oncoming traffic to avoid vehicles approaching from behind you.
- Avoid passing stationary cars with their engines running and people sitting in them.
- If you do have to walk in the same direction as the traffic and a vehicle pulls up suddenly alongside you, turn and walk or run in the other direction.
- Never accept a lift from a stranger or someone you do not know well, even if there is poor weather or you are late. Consider calling a friend or licensed cab.
- Keep your mind on your surroundings – remember if you are talking on your mobile phone or wearing headphones, you will not be aware of potential problems near you.
- Be particularly careful when using cashpoint machines. Make sure nobody is loitering nearby and do not count your money in the middle of the street.
- If you think you are being followed, trust your instincts and take action. As confidently as you can, cross the road, turning to see who is behind you. If you are still being followed, keep moving. Make for a busy area and tell people what is happening. If necessary, call the police.
- Try not to keep all your valuables in one place. It's a good idea to keep valuables such as wallets in an inside pocket.
- Consider carrying a personal safety alarm, which can be used to disorientate an attacker giving you vital seconds to get away.
- Let a friend know of your movements, planned routes, location and return time.

For further advice visit: **www.suzylamplugh.org**

Meetings and surgeries

Meetings and surgeries (e.g. MP/Councillor/GP)

When conducting meetings or surgeries, particularly where you may be alone in an office, you may meet people who are confrontational or in different states of distress. They may display different emotions and be upset, angry or aggressive. It is important to continually assess your surroundings, the person's behaviour and potential threats before and during meetings. You should take proportionate steps to reduce the risks and stay safe.

Ask yourself the following questions:

- Have I developed a plan for staff, outlining what to do in an emergency and have I reviewed it and tested it regularly with them?
- Is there an appointments system which identifies the visitor, location, start time, finishing time and ensures proportionate checks are conducted to reduce the risk?
- Is the designated surgery/meeting room close to other members of staff in case I need assistance?
- Are colleagues aware of where and when I am holding my surgery/meeting?
- Is there an incident log book that centrally and accurately records incidents? All types of unacceptable behaviour should be documented, dated, timed and signed. Anecdotal accounts can be unreliable.
- Has or is the visitor displaying signs of irrational, aggressive, or confrontational behaviour?
- Is it safe for me to conduct the surgery/meeting?
- Do I need to consider other options e.g. request a colleague to support me during the meeting or even call the police?
- Will my colleague check on me if the meeting takes longer than expected?
- Do they know how to contact me?
- Have I checked the room to make sure that it is set up correctly with no items lying around that could be used as weapons?
- Is my chair nearest the door, so that I can get out quickly if I need to?
- Do I have an escape route and have I identified a safe area for me and my staff?
- If I have concerns during the meeting how would I excuse myself without causing further issues?
- Have I planned a quick and safe exit if needed?
- How do I call for help if I need to?
- Have I agreed a key phrase to alert staff in the event I need assistance?
- Have I got my mobile phone with me, is the battery charged and can I get a signal?

Motor vehicles and travel

- Have I got a personal safety alarm with me and have I checked that it's working? These can be carried discreetly; they are designed to disorientate, giving vital seconds to get away.
- Is there a panic button facility in the room?
- Am I wearing appropriate clothing? A long scarf around the neck could be used to cause harm.
- Am I sat at their level?
- Am I using eye contact and open hand gestures to display a helpful attitude?

This checklist is not exhaustive, but should form part of your dynamic risk assessment. You may also consider having additional training to ensure that you have the necessary skills to deal with a potentially volatile situation.

Motor vehicles and travel

It is important to consider the security of any vehicles you use regularly; this includes personal and work usage. You may wish to consider alternative routes for regular journeys to reduce the predictability of your travel routines. Carry a fully charged mobile phone. For further advice and guidance refer to Suzy Lamplugh Trust: www.suzylamplugh.org

Vehicle security

- At home or in work, park your car in a locked garage or a secure parking area. If neither of these is an option, leave your vehicle where it can be seen by the general public. Try to park in a well-lit area, within view of a CCTV camera or in a staffed car park.
- When leaving your vehicle, ensure that the windows are closed and it is fully locked and secure.
- Be alert to any visual changes to your vehicle. If you notice a suspicious object on or near the vehicle, do not approach or enter it. Contact the police and give them the location and registration number of your vehicle.
- Carry a torch so you can check your vehicle after dark.
- Never leave laptops, documents, corporate clothing, parking permits or papers in unattended vehicles, as they may identify you or your employer.

Regular journeys

- If possible, avoid setting patterns in your travel arrangements which could make it easy for anyone to predict your whereabouts. Vary your routes and times of departure as much as possible.
- Make sure someone at home or work knows your route and the time you expect to arrive.
- Lock the vehicle doors and boot during your journey. Open windows only enough for ventilation purposes, particularly in town. Keep your distance from the vehicle in front.

- Do not run out of fuel! Always check you have the fuel required to complete your journey. Ensure you have adequate breakdown recovery cover.
- If you break down, pull as far off the road as you can and put your hazard warning lights on. Call your breakdown organisation and let them know if you are travelling alone or if you have children with you.
- If you break down on a motorway, it is usually safer to wait for assistance outside your vehicle, standing on the verge or behind the crash barrier. Take your keys with you and lock all doors except the one nearest to you, which you can leave wide open so that you can get in quickly if you need to.
- Make a habit of checking the road before leaving your home or place of work. Note any suspicious or strange vehicles and report them.
- If the driver of another car forces you to stop and then gets out of his/her car, stay in your car, keep the engine running and if you need to, reverse to get away.

If you think you are being followed:

- Try to keep calm.
- Keep the vehicle moving, even if only slowly.
- Close all windows and ensure doors/boot are locked.
- Contact the police immediately.
- If you can, make your way towards the nearest open police station.
- Do not drive home.
- Record the registration number of any suspicious vehicle.

Working away from home

Before travelling, make sure that someone at home knows:

- Your contact telephone number.
- Where you are going.
- Who you are going to see.
- How you will travel.
- When you expect to arrive and when you expect to return.
- What to do in the event of undue delay.

Public transport

Taxis

- If possible, do not use waiting taxis. Call and book ahead, so there is a record of your booking and the vehicle is properly licensed.
- Do not share a taxi with someone you do not know.
- Consider alternative pick-up or drop-off points to your home or place of work.
- Do not wear anything that would disclose your occupation.

Rail, sea, air and other public transport

- If travelling by train, enter a carriage that is already occupied. Keep luggage in view if you have to store it on a rack. Do not leave your possessions on your seat.
- Never leave your luggage unattended. Between packing your bags and check-in, maintain control of all items, both checked and carry-on luggage.
- If you have to surrender your luggage, make sure you get the right bags back. Do not open them unless you are confident they have not been tampered with. Secure zip loops with a padlock or use a lockable luggage strap.
- When travelling by ship, be cautious about walking on deck at night. Try to obtain a cabin and ensure that the door is kept locked at all times.
- Do not take responsibility for the luggage of people you do not know.
- Consider carrying a personal safety alarm with you.

Hotels

- Where possible, avoid regularly using the same hotel.
- At reception, try to avoid other people hearing your name and room number.
- Never see visitors in your hotel room. Meet them in a recognised place of business, in a public space or a meeting room (where venue staff will be aware of the arrangement).
- Be wary of hotel paging. It is advisable to prearrange with the hotel for callers to leave their name and contact details with reception. This will reduce the risk of identification and possible attack.
- Include a door wedge in your luggage.
- Know the fire and escape route options.

Delivered items and telephone threats

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, sharps or blades, or conceivably 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 well set it off. 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:

- Unexpected item, especially if hand delivered.
- A padded envelope 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 specific way.
- Oddly-shaped or lop-sided.
- Envelope flap completely stuck down.
- Marked 'To be opened by', 'Personal' or 'Confidential'.
- Item addressed to the organisation or a job title rather than a named person.
- Item addressed to a high profile individual.
- Unexpected or unusual origin (postmark and/or return address).
- Poorly or inaccurately addressed.
- Address printed unusually or unevenly e.g. using a lettering stencil. Unfamiliar style of writing.
- No return address or a return address that cannot be verified.
- Unusual postmarks or no postmarks.
- More stamps than needed for the size and weight of the package.
- Unusual smell.
- Greasy or oily stains emerging from within.
- Small hole(s) in the envelope or wrapping.
- Powders or liquids emanating from the package.
- Sudden onset of illness or irritation of skin, eyes or nose.

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. For further advice visit: www.cpni.gov.uk

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

- Note details about the caller: e.g. 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 etc.).
- Write down the details immediately; include date, time and exact words spoken, if possible. Keep a note pad and pen to hand.
- On termination of the call operate any trace facility, such as the BT 1471 service.
- Inform the police immediately if threats have been made.
- Consider making your home phone number ex-directory.

IT security and online communications

Tell your children to hang up without responding, if they receive such a call. You may decide that your children should not answer the telephone, if there is a risk of a malicious call.

Use a caller display function, so that the call can be screened before being answered.

If you are persistently receiving silent calls, do not say anything when you answer. Normal callers will identify themselves and if it is the malicious caller you can hang up.

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 On Line (www.getsafeonline.org) 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.

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 – online banking, personal emails, social media and photographs. Do you want these to be made public or used against you?

- Use all of the security facilities available, e.g. 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 is on the phone box package, under the phone battery or can be found 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 if appropriate 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.

IT security

- Use a firewall and anti-virus software and keep them up to date. Run system scans regularly.
- Be cautious when using third party applications. Malicious codes known as 'malware' can spread rapidly around social networks or via email.
- Do not open emails from unknown or suspicious senders.
- Treat all email attachments and links with caution. Where it exists, turn off the option to automatically download attachments to emails.
- Use software controls that ensure only reputable websites can be accessed, reducing the risk of malicious software being installed on the system.
- Make sure that the latest updates to your device's operating system are promptly installed.
- Check the security protection of your home/business Wi-Fi networks. Change the default (manufacturer) passcode.
- Use a hard-to-guess password and never write it down. Do not tell anyone your password.
- Do not use the same password for all security log-on purposes.
- Shred CDs/DVDs before disposal if they contain sensitive information.

Children's personal safety online

Information and support for young people/parents and professionals is available on the education website at: **www.thinkuknow.co.uk**

Child Exploitation and Online Protection Centre (CEOP): **www.ceop.police.uk**

Protest activity

Online Social Networking (OSN)

The internet can be a valuable source of information, education and entertainment for all the family. However, you need to take precautions when using it, especially for social networking purposes.

Internet-based social networking sites such as Facebook, Twitter, LinkedIn and Instagram are popular applications that allow individuals to create a profile containing personal information and interact with other users. Review your privacy settings otherwise some or all of your OSN profiles can be seen by a large audience.

Business networking sites, such as LinkedIn, also require personal profiles to be created which normally include an individual's work history. Whilst these applications are useful tools to communicate with others or advertise your professional skills, publishing personal information on your OSN profiles presents potential risks:

- You may be susceptible to identity theft, as dates of birth, full names, home addresses and email details are key pieces of information for identity fraudsters. Some sites 'own' any data posted on them and may reserve the right to sell your details to third parties.
- Posting information can put your personal safety at risk. If you provide too much information and do not have the appropriate privacy settings applied, your business or social network accounts can be a veritable 'gold mine' for those intent on building up a picture of your relationships, opinions, places of interest and any other subject that they may seek to exploit in the future.
- Location-based information can be posted on social networks, especially from GPS-enabled mobile devices, which tells others exactly where you are or have been. This information is not secure and could be viewed by anyone, including those who may want to harm you or your family, friends and colleagues. The responsibility rests with you to ensure that no-one is put at risk due to what is disclosed.
- Regularly check what information you can find out about yourself, your family or your business on-line and edit where able.

You should not include personal details such as:

- Mobile phone numbers.
- Personal or work addresses.
- Employment details.
- Family members.
- Hobbies and places frequented.
- Vehicle details.
- Work information on personal accounts.
- To avoid putting other people at risk, photographs of family, friends and colleagues should only be published with your consent and theirs. If applicable, published photographs should not reveal your occupation, home or place of work.
- Review your account settings. Disable photo and location tagging, so you have to approve another user identifying you in a photograph or being at a specific location. Ensure your privacy settings are adequate and your account is as locked down as it can be.
- It is equally important that family and friends are made aware of any risk, in order for them to take suitable precautions with their online presence. This is especially relevant if they are used to posting content about the person 'at risk'.

Demonstrations

It is possible that your profession or association with an organisation could lead to protesters gathering at your home or work. They may assemble close to the boundary of your home, work place or even on your property.

If this happens:

- Stay calm – such protests may intimidate but will not necessarily lead to a physical threat.
- Remain inside.
- Close and lock doors and windows and draw the curtains/blinds.
- Inform the police using the 999 system.
- Inform your workplace/colleagues.
- Do not, in any way, respond to or antagonise the protesters; remain indoors out of sight and avoid confrontation.
- If possible, note descriptions of individuals and vehicles present.
- If you have a CCTV system fitted that has recorded images of protesters, you should hand any footage obtained over to the police; it may assist with identification and provide evidence in cases where offences have been committed.
- Postpone any expected visitors.
- Wait for the arrival of police.

Publicity and the media

Leafleting campaigns

Your neighbours may receive letters or leaflets describing in extreme terms the work that you do. Most people, whatever their personal view on the subject at issue, will be sympathetic towards anyone who is being victimised.

- You may want to talk to your neighbours.
- All incidents should be logged and reported to police and to your employer.
- Do not remove any posters or offensive notices found on your property without prior, careful examination.
- Leaflets or other materials should be passed to police.

Avoid revealing details about personal circumstances which might be of use to a person planning to target you or your business interests. This includes interactions with the media, be it for work or social purposes. It is impossible to provide advice to cater for every eventuality but the following are some examples of the kind of publicity which should be avoided or controlled:

- Home addresses and other identifying details should be excluded from business publications and online networks.
- Work related press releases, publicity materials and website content should be reviewed to see if any information can be removed or amended to protect individuals.
- Television camera crews and press photographers should not generally be allowed to enter private homes. However, where agreement is reached to grant interviews to the press on private premises or to the publication of articles about the private lives of interviewees or their families, the media should be asked not to publish details which would help to identify a home address or regular way of life.
- The electoral role is a source for commercial companies to obtain your personal information. You can seek advice on how to protect this information from your local authority.
- If you have professional membership of any business-related organisation, ask them not to publish your full details or, if they do, to put them on a password-protected area of the site.

In the event of an attack

If, in spite of the precautions you have taken, an attack has been made or attempted, it is essential that:

- Police are alerted immediately.
- You follow their instructions absolutely.
- Nothing is touched at the scene.
- No information is given, other than to the police.

Useful websites

Security advice

National Counter Terrorism Security Office:
www.gov.uk/government/organisations/national-counter-terrorism-security-office
Centre for Protection of the National Infrastructure: www.cpni.gov.uk
Foreign Travel advice: www.gov.uk/foreign-travel-advice

General crime prevention advice

Secured By Design: www.securedbydesign.com
Anti-fraud advice: www.actionfraud.police.uk
Sold Secure: www.soldsecure.com
Master Locksmith Association (MLA): www.locksmiths.co.uk

Personal safety advice

Crimestoppers: www.crimestoppers-uk.org Tel: 0800 555 111
Suzy Lamplugh Trust: www.suzylamplugh.org
Victim Support: www.victimsupport.org.uk

Cyber/Information security advice

Get Safe Online: www.getsafeonline.org
Cyber Street: www.cyberstreetwise.com
Internet Security & Safety Advice: www.knowthenet.org.uk
Advice on how to help children use the internet safely: www.internetmatters.org
Child Exploitation and Online Protection Centre (CEOP): www.ceop.police.uk

Direct marketing removal

Mail Preference Service: www.mpsonline.org.uk
Telephone Preference Service: www.tpsonline.org.uk
Local Police Station:
Local Counter Terrorism Security Adviser:
Local Hospital:
Local GP Surgery:

'If you suspect it report it'

0800 789 321

Confidential Anti-Terrorist Hotline

In an emergency dial 999

Non emergency calls dial 101