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 system.

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. Don't make their job easier through complacency.

Identifying vulnerability

Vulnerability means openness to 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 'red alert' 24 hours a day. The information in this booklet will help you decide where you need to take precautions, when to maintain the highest level of alert and when you should involve the police.

Security at home

Good personal security extends beyond work to your 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.

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. Consider growing trees or shrubs near your boundary to hinder access to your garden. However, control the growth of vegetation to eliminate hiding places.
- Garages, outhouses and garden sheds should be kept locked when not in use. Check garage doors and windows each morning for signs of forced entry.
- If possible, keep your dustbin/recycling bin in an enclosed yard. Nothing of a sensitive, confidential or personal nature should be placed in the bin.
- 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.
- Remove objects that could be used as missiles: for example, loose bricks, large stones and garden ornaments.
- Do not remove any posters or offensive notices found on your property without prior, careful examination.

Doors, windows and locks

- Ensure good quality locks are fitted to external doors and access windows.
- Establish a routine for completing checks to confirm all doors and windows are secure, e.g. before going to bed or leaving the house.
- Fit a cable guard or strong door chain on outer doors. Make sure you use it.

- Fit an appropriate letter guard.
- A video door phone or an intercom will enable you to identify callers before you open the door. Even then, only open the door with the chain or limiter still in place.
- Know where all your door keys are. Do not hand keys out to builders, tradespeople etc.
- If you cannot account for all keys, change door locks.
- Obscure the view into your home by fitting blinds or curtains, including glazed exterior doors. Get into the habit of closing curtains or blinds when occupying a well-lit room.
- Make sure the keys for windows which could be used to exit the building in the event of a fire are kept to hand. They should not be visible or within reach from outside.

If you replace doors, windows and security products, ensure they have been tested to withstand attack and meet one of the following standards: PAS 24:2012, STS 201 or LPS 1175 SR2. – for further guidance see Secured By Design: www.securedbydesign.com

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.

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 available for emergencies.
- Fit a burglar alarm or intruder detection system. Set external sounders at 'instant' to deter intruders if the alarm or a personal attack button is activated.
- Intruders do not want to be seen or heard so setting off an alarm and attracting attention is their enemy. To maximise the deterrent, place externally active burglar bell boxes (with flashing lights and sounders) at the front and back of the property. Police recommend an installer who is affiliated to an inspectorate, such as National Security Inspectorate (NSI) or Security Systems and Alarms Inspection Board (SSAIB). Be aware that DIY alarms will not necessarily receive a police response.

Lighting

- Good external lighting can help to deter intruders.
- Consider lighting the approaches to your home and outlying buildings with exterior lights sited out of reach. In most cases, the preferred and cost effective security lighting are continuous ambient lighting, low wattage bulbs activated by photo-electric cell which will automatically switch on from dusk till dawn. The alternative of passive infra-red lights can be accidentally triggered by pets or wild animals and must be thoughtfully positioned to avoid being annoying to neighbours. Manual override switches allow complete personal control.
- Install an illuminated 'courtesy' light, operated by a sensor in the area of the front door.
- Always have reserve lighting, such as a torch, lamps or candles, at hand.
- 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.

CCTV

- Seek further advice from a professional accredited to NSI (National Security Inspectorate) or SSAIB (Security Systems and Alarm Inspection Board)

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.

If you are suspicious, do not open the door. If you feel that you are under immediate threat, call 999.

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 it is fully locked and secure with windows fully closed.
- 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 the vehicle. Contact the police telling them your vehicle registration number.
- Carry a torch so you can check your vehicle after dark.
- Never leave laptops, documents, corporate clothing, parking permits or papers in unattended vehicles, that 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.
- Don't 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.

Delivered items and telephone threats

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 don't know.
- Consider alternative pick-up or drop-off points to your home or place of work. Don't 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. Don't 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.
- Think about carrying a personal 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

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 or incendiary (the two most likely kinds), or conceivably contain chemical, biological or radiological material. Other hazardous substances, 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. However, any attempt to open such an item may well set it off. Unless delivered by a courier, it is unlikely to contain a timing device.

Devices contained within delivered 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:

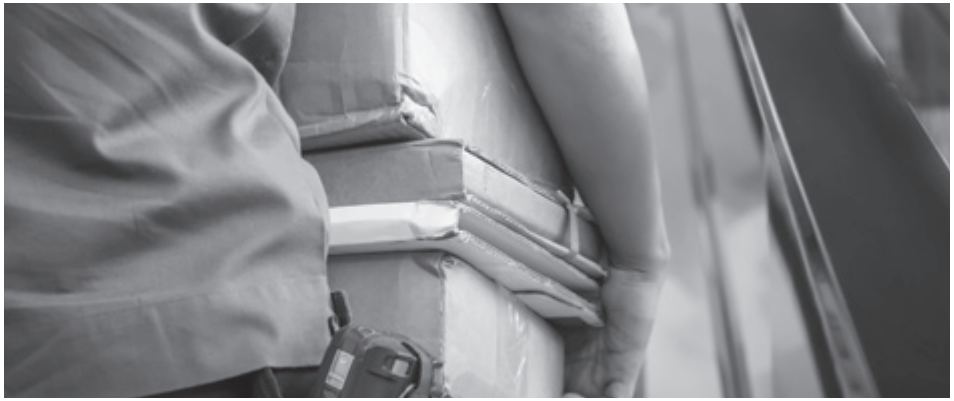
- Unexpected item, especially if hand delivered. A padded envelope or other bulky package.
- An additional inner envelope or other contents that may be difficult to remove.
- Labelling or excessive sealing that encourages opening at a particular end or in a specific way.
- Oddly-shaped or lop-sided.
- 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.
- 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.

IT security and online communications



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.

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 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.

Online Social Networking (OSN)

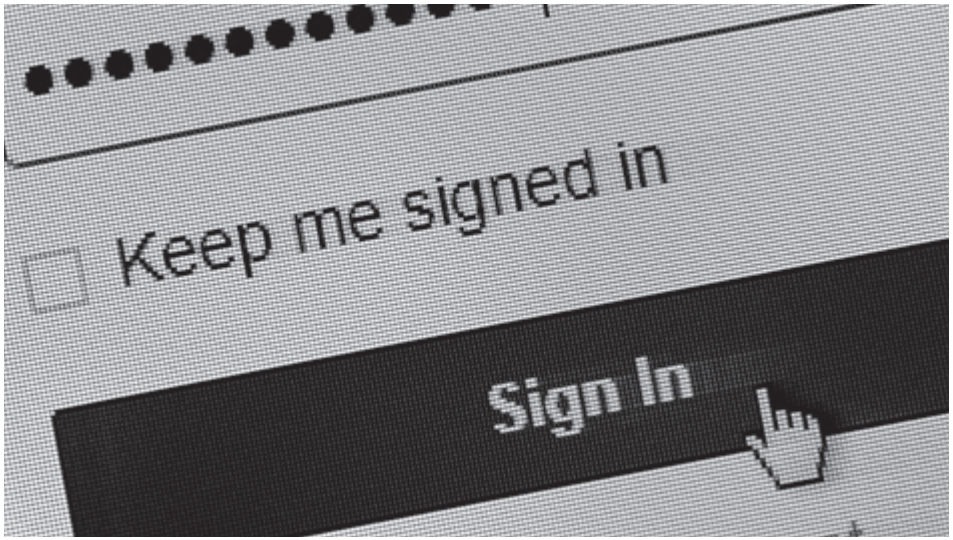
The internet can be a valuable source of information, education and entertainment for all the family. However, you need to take precautions when using it, especially for social networking purposes.

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 profile 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, there are risks associated with the use of these sites.

Publishing personal information on your OSN profiles presents two 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'.

Protest activity

Demonstrations

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

If this happens:

- Stay calm – such protests may intimidate but will not necessarily lead to a physical threat.
- Remain in your home.
- Close and lock doors and windows and draw the curtains.
- Inform the police using the 999 system.
- Inform your workplace/colleagues.
- Do not, in any way, respond to or antagonise the protesters; remain indoors and out of sight. 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.

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.
- Leaflets or other materials should be passed to police.

Publicity and the media

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 the 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.org.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

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

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 Surgery:

'If you suspect it report it' 0800 789 321
Confidential Anti-Terrorist Hotline