ProtectUK

Personal security

Original publication date
02/11/2020

1. Introduction

The more you do to protect yourself, the safer you and your family will be. There are three key areas which can affect your safety. These are physical security, situational awareness/security, and online security. This document does not provide definitive advice in all of these areas, but instead provides general guidance along with links to more detailed security guidance, which you may wish to read.

2. Assessing an appropriate level of protection

This guide provides generic advice on how to stay safe at home, at work, on-the-move, and online. Exactly which measures you adopt will depend on the extent, or level of threat you are likely to encounter and the vulnerabilities you have.

To help assess this you should consider the following:

- your profession/role – 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?

No-one has more responsibility for your personal security than you. Today, individuals face a range of potential threats – from criminals to extremists. Good personal security should take into account both your work and home life and any 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.

This guidance will help you decide where you need to take precautions, when to maintain heightened awareness and when you should involve the police. No one can be on high alert all the time, but being complacent may expose you to vulnerabilities.

Here are some effective measures you can take. This list is not exhaustive and the precautions you use will depend on individual circumstances.

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, how to be on your guard. Attackers can be creative when it comes to finding ways and means to target individuals and their families. Their objective may be to cause embarrassment, inconvenience and distress, but may also include the intent to cause physical injury or threaten life itself.

3. Physical security

Security at home – house and grounds, doors, windows, locks, keys, alarms, lights and CCTV.



There are a number of simple measures you should consider to protect yourself and ensure your home is secure. Protection starts with the perimeter of your property; any fences or walls should be well maintained. It is important that boundaries clearly define the difference between public and private space. Make sure tools and ladders, which could be used to access your home, are locked away and remove anything that could potentially be used to cause damage, such as loose bricks, large stones and garden ornaments.

Make sure good quality locks are fitted to external doors and windows. Remember to keep house keys out of sight, but in a secure place in case of fire. Do not label your keys. If you need to identify keys use a colour-code theme. If you cannot account for all your keys, change the locks.

If you have an alarm installed, you should 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). A monitored alarm may be more expensive, but it will cause a response to be undertaken by the alarm company, whereas a purely audible alarm relies on neighbours and passers-by to react.

You should make sure you have good external lighting covering external doors, car parking areas

and footpaths leading to your home. Consideration should be given to the fitting of floodlights at strategic points to make it difficult for would-be assailants to hide from view. If you consider installing CCTV, seek advice from a professional CCTV installer accredited to one of the recognised CCTV inspectorate bodies, such as the NSI or the SSAIB.

If you cannot park your car in a locked garage or a secure parking area, then 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. Always make sure the windows are closed and the car is fully locked and secure.

Go to the Secured by Design website.

4. Situational awareness/security

Weapons and firearms attacks

Marauding Terrorist Attack: **RUN HIDE TELL** covers advice on actions to consider in the event of a weapons or firearms attack.

Visitors

Always clearly identify callers to your home before letting them in, and check the identity of tradespeople on their arrival. Never leave them alone in the house. Teach children never to answer the door or let strangers in to your home; .tell them to fetch an adult to do it.

Confidential waste

Always treat sensitive, confidential or personal material you are disposing of as confidential waste. Shred it and/or burn it. If shredded at work, put it in a confidential waste bag and keep it safe, not in a public area, until it can be disposed of correctly.

Street safety

Personal safety should always be a key consideration when travelling. By taking suitable precautions,

you can reduce the opportunity, and therefore the risk, of experiencing violence or aggression. Consider simple measures such as planning ahead before you go out, taking the safest route, and avoiding danger points like quiet or poorly lit alleyways or isolated car parks.



When out, if you are at all worried, try and stay near a group of people. Whenever possible, walk facing oncoming traffic to avoid vehicles approaching from behind you. Never accept a lift from a stranger or someone you don't know well, even if the weather is poor or you're late. Keep your mind on your surroundings – if you are talking on your phone or wearing headphones, you will not be aware of potential problems near you. Be particularly careful when using cash machines. Make sure nobody is loitering nearby and do not count your money in the middle of the street. Consider carrying a personal safety alarm, which can be used to disorientate an attacker giving you vital seconds to get away.

Go to the Suzy Lamplugh Trust website.

Meetings and surgeries

If you are an MP, Councillor or a GP for example, you will have to conduct meetings or surgeries.

You may be alone in an office or 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.

Motor vehicles and travel

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. 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. You should always check you have the fuel required to complete your journey.

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 and report any suspicious or strange vehicles.

If you think you are being followed, try to remain calm and keep your vehicle moving, even if only slowly.



Close all windows and make sure that your doors and 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.

Anonymous telephone calls and threats

These are usually intended to cause fear, alarm and distress. These calls can be extremely distressing but, if it is bearable, keeping the caller talking can reveal important information. It is a criminal offence to make threatening or abusive telephone calls and you should consider contacting the police.

Go to the Ofcom Abusive and Threatening Calls webpage

Go to the Ask the Police website.

5. Online security

Use of mobile devices

Mobile devices can hold a variety of personal details such as online banking, emails, diary, contacts, social media and photographs. To keep your device secure, you should use all its security features. These include setting up device tracking and creating screen and SIM pass codes. Switch off GPS tracking when it is not required.

An IMEI is a unique 15-digit serial number which can be used to identify a lost or stolen phone or mobile enabled tablet. Keep a record of your device's IMEI number. IMEI number can be on the back of a device, under a removable battery or on the device's original packaging. You can also get it by typing *#06# into your phone.

Always change the default PIN for voicemail access. Avoid using public Wi-Fi hotspots as they may not be secure. You should consider disabling location services on your phone, 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 which can reveal private information to a third party. Remove metadata from pictures, especially ones taken from mobile phones before you post them online.

Safely using the internet and managing personal information online

The internet can be a valuable source of information, education and entertainment. However, you should take precautions online with the amount of personal information you publish, especially for social networking purposes.

Online Social Networking (OSN)

Popular sites, such as Facebook, Twitter and Instagram, allow individuals to create a personal profile and interact with other users online. Additionally business networking sites, such as LinkedIn, also require personal profiles to include an individual's work history.

Whilst these are useful tools to communicate with others or advertise your professional skills,

publishing personal information online 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. In addition, information regarding employment, personal or work addresses, family members, hobbies or vehicle details are also extremely valuable to criminals and other potentially hostile parties. Some social networking sites own any data posted on them and may reserve the right to sell your details to third parties.

You should regularly review your privacy settings for these sites otherwise some or all of your personal profiles could be seen by a large audience unknown to you. Additionally, your family and friends can innocently divulge information about you if they do not take appropriate measures to protect their profile information.

Go to the NPSA (formerly CPNI) Online Social Behaviour webpage.

Doxing

Doxing is the practice of researching and publishing private or identifying information about a particular individual on the internet. Online research is used by a wide group of terrorists and hacktivists alike to harvest information on individuals. This can then be used to incite fear in target populations and individuals, and therefore satisfies some terrorist objectives.

Posting information online 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 provide a lot of useful information 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.

Go to the National Cyber Security Centre website.

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 curtains/blinds. Call the police on 999.

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.

KEYWORDS
PERSONAL SECURITY

SOCIAL MEDIA
SECURITY
CYBER
CYBER SECURITY
PALS GUIDANCE
PUBLICLY ACCESSIBLE LOCATIONS