Looking after your personal security and privacy
A drivers guide from Alphabet

The face of car crime has changed dramatically over recent years. Vehicle manufacturers have made their cars and vans harder to steal, leading criminals to change their tactics. Today the fastest growing risk to drivers is cybercrime of one kind or another. That doesn't mean that longstanding issues like opportunistic theft or risks to personal safety have gone away though.

This guide looks at the risks that every driver should know about across the following areas:

– Cyber security and privacy
– Personal safety
– Vehicle security

Within each area we describe the common threats, suggest the actions you can take to avoid falling victim to them and offer advice on what to do if it does happen to you.

1. Cyber security and privacy

In-car data risks

Your modern car is a highly sophisticated electronic and mechanical device. A typical high-end car contains around 100 million lines of computer code, which is twice as much as the Large Hadron Collider and eight times more than the software in a Boeing 787 Dreamliner.

Today's cars allow you to connect phones and other devices to the infotainment console, or to login to social media and other cloud-based services. More and more cars link remotely to their manufacturer to transfer maintenance information or download software updates.

While this trend has led to high-profile speculation about hackers potentially gaining control over connected cars, the more-likely scenario is that someone might access your car's systems to obtain personally-identifiable data about you.

For example, when you pair a phone with your car via Bluetooth, the default setting is usually to import all the phone's call logs and contact data. That's very convenient for staying connected on the move but it adds to the risk that someone could get their hands-on information they could then use to steal your identity or scam people you know.

Continues Over »

How can I secure my onboard data?
Protecting your in-car data privacy is mainly about knowing how to clear personal data when the time comes to change your car – or if you are very privacy-minded whenever you hand it over to someone else, such as for servicing you should:

– Delete addresses, call logs, texts, etc.
– Clear destinations and trip logs from the sat nav
– Disconnect from any social media networks
– Do not leave documents giving your name and address – e.g. copies of service receipts – in the vehicle

Online safety for drivers
Tens of thousands of people fall victim to online scams every year, with two types of website in particular targeting drivers.

'Impostor' sites try to get you to pay for something which is actually free of charge or much cheaper than if you go to the genuine web site.

Examples are European Health Insurance Cards (EHICs) and Crit'air emissions stickers for driving in Paris and certain other French cities. These Crit'air stickers cost very little at £3.50, from the genuine sites (www.ehic.org.uk and www.crit-air.fr). However, web search results may feature sites that charge £30 or more to 'administer' your application. It's not illegal to charge for reviewing or forwarding applications but these sites are carefully designed and worded to disguise the fact that they are merely an unnecessary and expensive intermediary.

Other driving-related tasks known to be targeted by "impostor" sites are driving licence renewals, theory test applications and congestion charge payments, all of which are operated by unscrupulous people which trick drivers into paying for an intermediary service they don't need to use.

Scam or phishing sites also masquerade as genuine sites however the people behind them are out to steal your financial and identity information, or trick you into installing ransomware, forcing you to pay hundreds of pounds to unlock your computer. As these sites are illegal, search engines quickly block them so the scammers usually draw their victims in by phone, text or email. One widely-used scam asks people to pay a 'driving licence verification fee' at a site purporting to be the Driver and Vehicle Licensing Agency. Scam sites look genuine but the payment is unnecessary (there's no such fee) and the scammers then can sell your payment card details to other criminals.

How to avoid online scams
Virtually all official driving-related matters, from driving licences to road tax to vehicle registrations are handled by UK government agencies. If you're in any doubt about where to go, start at www.gov.uk, the government website and use the search box or the 'Driving and Transport' link on the homepage. You should avoid using a commercial search engine.

Phishing scams rely on catching people with their guard down. The scammers deliberately send out millions of blatantly obvious scam messages in the hope that one of them will slip under your radar. Alertness and knowledge are your best defence against this risk; together with installing reputable cybersecurity software.

A great free knowledge resource is Get Safe Online www.getsafeonline.org, a partnership supported by HM Government and leading organisations in banking, retail, internet security and other sectors. It offers a wealth of advice on how to avoid falling victim to cybercrime, as well as information on what you can do if it happens to you.

If it happens to you
Unfortunately, once you've handed over money or personal details to online fraudsters, your chances of getting anything back are very small. You can try asking impostor sites to return your money but you'll have legally committed to the payment when you agreed to their terms and conditions during checkout. You could take the owners to the small claims court but, even if you win, the procedure will probably cost you more than you paid the site.

If you're a victim of ransomware, the National Crime Agency's advice is **do not pay the ransom**. Go to the No More Ransom (www.nomoreransom.org) project, which offers decryption keys for many different types of ransomware.

Whatever type of online fraud you encounter, report it to Action Fraud (www.actionfraud.police.uk), whose website also provides links to organisations that can help victims.

Continues Over »

2. Personal safety

Amid all the attention given to online security, criminal risks to drivers' physical safety shouldn't be overlooked. Thankfully, most drivers rarely if ever need to worry about a criminal risk to their own safety. Nevertheless, it pays to be aware of potential risks and to take precautions against them.

Plan ahead
Getting lost at night or breaking down in unfamiliar surroundings are two very common fears. Before setting out, check your fuel, oil and tyres. Make sure your sat nav is up to date or you have a current road atlas and, if you are travelling after dark, make sure someone knows your destination and expected arrival time. Keep some coins in the car for parking or if you have to make a call and there's no mobile signal.

Pick a safe parking place
Always aim to park in a busy, well-lit area, especially if you expect to return to your vehicle after dark. Look for the Park Mark badge on car parks - it means they have passed a police inspection for standards of cleanliness, layout, lighting and surveillance. Make a habit of reversing into parking spaces: you'll be able to get away quickly if you need to. Have your keys in your hand as you approach your car so you can unlock it, get in and drive off without delay.

Don't tempt fate (or thieves)
Keep your doors locked even when driving, especially in traffic and built up areas where an opportunist could reach in to grab valuables or even force you from your vehicle. Put handbags and laptops in the rear passenger foot well or boot while driving but never leave valuables in your car overnight, particularly at hotels as thieves are known to target business travellers.

Harassment by other drivers
Despite a few lurid headlines in recent years based on unofficial surveys, harassment or actual attacks on other drivers are comparatively unusual. However, should you find yourself in a potentially threatening situation, police advise you to:

– Stay in your car with the windows closed and doors locked.
– Avoid getting involved in an argument or intervening in a 'road rage' incident you may witness.
– If the driver or passenger in a car next to you at a junction or a traffic lights tries to attract your attention, ignore them and don't make eye contact. It may be a genuine warning but don't stop or get out of the car until you can pull into a busy public place such as a garage forecourt, supermarket or pub.
– The same applies if you think someone is following you or deliberately trying to intimidate you. Drive to a busy place and only unlock your doors when you are confident there is no danger. If you are sure you face an imminent threat, call 999 (an emergency is the only time it is legal to use a phone while driving). Try to make a mental note of the colour and type of the other vehicle or better still its registration but your priority should be to ensure your safety.

If someone forces you to stop
If a car pulls in front of you and forces you to stop, leave the engine running. If the driver, or passenger gets out and approaches you:

– Make sure your doors are locked and the windows closed
– Turn on your hazard lights
– Reverse as far as you can and sound your horn continuously, no matter what time it is

If it happens to you
Report the crime to the police, even if you can provide little or no information that might identify the perpetrator(s). If you were driving on business at the time, report the incident to your company.

3. Securing your vehicle

Although vehicle thefts in the UK had fallen to their lowest level in nearly 50 years, thieves still stole nearly 66,000 vehicles in 2013. Since then, figures from the RAC have unfortunately shown a 30% increase in car theft between 2013-16. Car criminals are learning to adapt computer hackers' tools and know-how to defeat even the most up-do-date anti-theft measures. As a result, modern keyless entry and ignition systems have become a 'key' target for thieves.

Continues Over »

Four tools used by car key hackers

'Sniffer' devices intercept and read the coded signals between the key fob and the car when the driver opens or locks it. One hacker has shown off a device that can even crack 'rolling' security codes that change every time the car is opened.

Booster or Relay devices amplify the car-to-fob signal. This fools your fob into opening the car even when you are sure it's safely out of range of the vehicle. The thieves repeat the trick to start the engine.

Jammers block the signal as the driver presses the locking button on the fob, leaving the car unlocked. Using a device that plugs into the car's diagnostic port, it takes the thief seconds to re-programme a blank key fob to start the engine.

App hijacking targets apps that let owners unlock their cars with their phone. If the thief can steal or guess your app password, they can log into it on their device to get into your vehicle.

How to Counter keyless crime

Be vigilant when you are getting in and out of your vehicle. Look out for anyone loitering suspiciously. Always listen for the sound of the locks operating when you press the fob. Lock the doors while you are still close to the car, not while walking away, and give the door handle a tug if in doubt.

Some sources advise keeping your fob in the fridge or microwave at home to shield it from sniffers or boosters. In practice, a metal box or a pouch lined with cooking foil should be sufficient – or you could buy a purpose-made signal-proof key store.

Invest in a physical anti-theft device such as a steering wheel, pedal or gearshift lock. These are by no mean infallible but they are likely to persuade a would-be thief to look for an easier target.

Finally, talking of keys, it's an idea to look in your vehicle's handbook to check what the remote-locking buttons do. With some keys, one press engages the locks and alarm; you press again to engage the deadlocks too. On others, a single press engages the alarm and deadlocks but a double press turns the alarm off again.

Key theft

It's not all electronic warfare. Thieves are now more focused than ever on physically getting hold of vehicles' keys and fobs. Every year, many cars are taken from driveways by thieves who use simple wires and hooks to fish keys through the owner's letterbox. Cafes, changing rooms and even offices also offer easy pickings when people leave their keys and handbags in plain sight.

Really ruthless thieves simply try to force a driver out of their car while the keys are in the ignition. Car-jacking is still rare but all drivers should follow advice about always keeping their car's windows shut and doors locked in stop-start traffic. Be alert when entering or leaving your vehicle; if in doubt, lock the doors as soon as you're inside, even before you insert the ignition key.

Police advice on securing your vehicle

The Home Office's police.uk website recommends that the best way to protect your vehicle and your belongings is to lock your car whenever you leave it.

Protect your belongings

– Removing everything from the car; don't even leave a jacket where it can be seen
– Closing the sunroof along with the windows when you leave
– Not storing things in the boot; take them with you
– Storing car ownership information in your home, not your car
– Having a routine to ensure you always take the keys out of the ignition
– Taking removable stereos and sat nav equipment with you
– Ensuring charging cables for phones or sat navs are stored out of view. The sight of a sat nav charger is often enough for a thief to break into a car.

How to keep your vehicle safe at home

Keep your keys away from doors and windows, and tucked away out of sight.

Have your vehicle's windows etched with its registration number or the last seven digits of the vehicle identification number (VIN). This can put criminals off, as it makes your car more difficult to sell. It also makes it easier for police to get your car back to you if it is stolen.

On cold mornings, clear the glass with an ice scraper before unlocking the doors, then get in and drive off immediately: it's less risky than leaving the car with the engine running to defrost the glass - you're unlikely to be insured if you leave your car running plus you'll save fuel.

Continues Over »

Vehicle cloning

Cloning a vehicle by fitting its number plate to another is the automotive version of identity theft. Your car's plates may be physically stolen or someone may use forged documents to get copies made. The first you're likely to know about it is when you start receiving penalty charges and speeding tickets for offences involving the other vehicle. Police and prosecutors are aware of the issue and will give you a sympathetic response but the process of proving your vehicle really has been cloned and re-establishing its identity is likely to be long and tedious. You'll need to:

– Return any fines or correspondence to the issuing authority, providing them with any documentary evidence to prove your case.
– Inform the DVLA. They will record your correspondence on the vehicle record for future reference.
– Contact the police. They can trace and prosecute the culprit to prevent this illegal activity from continuing.

Fitting theft resistant number plates can make your plates less attractive to thieves

Update your vehicle's security

Although factory-fitted anti-theft features are generally excellent, you can make your vehicle still more crime-resistant by fitting additional security equipment. Make sure it's approved by Thatcham Research (www.thatcham.org), who test both original equipment and aftermarket security products including electronic and mechanical alarms and immobilisers, wheel locks and tracking systems. You may get a discount on your insurance premium if you fit a Thatcham approved product.

If it happens to you

Tell the police and your insurance company straight away if your vehicle has been stolen. If it's a company vehicle, call the relevant number in your fleet handbook.

Check the streets and parking places close to where the vehicle disappeared. Thieves are known to "pinch and park" cars to see whether they are fitted with a tracker. If the car is still there after a few days, the culprits reason "it's not tracked so they can safely drive it away without leading the police straight to them".

When reporting the theft to the police, dial 101 and ask to be put through to your local police. They'll ask you for the vehicle's registration number, make, model and colour. You'll get a crime reference number to give to the insurance company. If the vehicle isn't recovered and the insurance company pays out, you must tell the DVLA.

More information

www.roadwise.co.uk

www.365alive.co.uk/cms/content/drivers-and-passengers

www.cyberaware.gov.uk

www.nationalcrimeagency.gov.uk

www.victimsinformationservice.org.uk

www.mygov.scot/victim-witness-support

www.gov.uk/what-to-do-if-your-vehicle-has-been-stolen

If you have any questions please contact us on 0370 50 50 100

Alphabet (GB) Limited, Alphabet House, Summit Avenue, Farnborough, Hampshire, GU14 0FB. Tel: 0370 50 50 100.
Registered office address: Alphabet House, Summit Avenue, Farnborough, Hampshire GU14 0FB. Registered in England and Wales 03282075.
Alphabet (GB) Limited is authorised and regulated by the Financial Conduct Authority.

ALMAR 025.2
Expiry 29.04.20