

# Situation Report

## Security & Safety

### Current Threat Level

#### International threats

The threat to the UK (England, Wales, Scotland and Northern Ireland) from international terrorism is **SEVERE**



**CURRENT UK  
THREAT LEVEL:  
SEVERE**

#### Northern Ireland-related threats

The threat to Great Britain (England, Wales and Scotland) from Northern Ireland-related terrorism is **MODERATE**.

The threat to Northern Ireland from Northern Ireland-related terrorism is **SEVERE**

You can check the current threat levels:

- [in the terrorism and national emergencies](#)
- [on the MI5 website](#)

The most significant terrorist threat comes from international terrorism. As a number of recent European attacks have showed, attacks may be mounted without warning.

Northern Ireland-related terrorism continues to pose a threat. Dissident republican terrorist groups (such as the Real IRA and the Continuity IRA) have rejected the 1998 Good Friday Agreement. They still aspire to mount attacks within the UK mainland and have conducted attacks within Northern Ireland.

**5 CATEGORIES OF RISK**

- CRITICAL**  
An attack is expected imminently
- SEVERE**  
An attack is highly likely
- SUBSTANTIAL**  
An attack is a strong possibility
- MODERATE**  
An attack is possible but not likely
- LOW**  
An attack is unlikely

## Stay Safe

Attacks in the UK and abroad remind us all of the terrorist threat we face. Police and security agencies are working tirelessly to protect the public but it is also important that communities remain vigilant and aware of how to protect themselves if the need arises.



### 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 cannot 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 / heavy reinforced walls
- Be aware of your exits
- Try not to get trapped
- Be quiet, silence your phone and turn off vibrate
- Lock / barricade yourself in
- Move away from the door

## TELL

Call 999 - What do the police need to know? If you cannot speak or make a noise listen to the instructions given to you by the call taker

- 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



**COUNTER  
TERRORISM  
POLICING**

**ACT**

**ACTION  
COUNTERS  
TERRORISM**

**IN THE RARE EVENT OF  
a firearms or weapons attack**

**RUN HIDE TELL**



**RUN** to a place of safety. This is a far better option than to surrender or negotiate. If there's nowhere to go, then...

**HIDE** It's better to hide than to confront. Remember to turn your phone to silent and turn off vibrate. Barricade yourself in if you can. Then finally and only when it is safe to do so...

**TELL** the police by calling 999.

## Stay Safe - Abroad this Summer

Wherever you're travelling this year, CT Policing and The Travel Association ABTA want you to join the seven million people who have watched vital safety advice that could save your life.



The UK's most senior counter terrorism officers are reminding holidaymakers to play their part in our collective security by watching the 'Run, Hide, Tell International' video, a tutorial of how to react in the event of a gun or knife terror attack.

ABTA have translated it into 15 different languages for use in multiple countries, to improve awareness amongst the holiday representatives, hotel staff and security guards who look after millions of UK tourists every year.



The FCO also advises holidaymakers to read the [FCO - Travel Advice](#) and to sign up for email alerts to be notified of any updates for their destination, either before or during travel. Travel advice provides objective information and advice to help people make better-informed decisions about foreign travel.

## Crowded Places Guidance

The UK faces a real threat from terrorism and crowded places remain an attractive target.

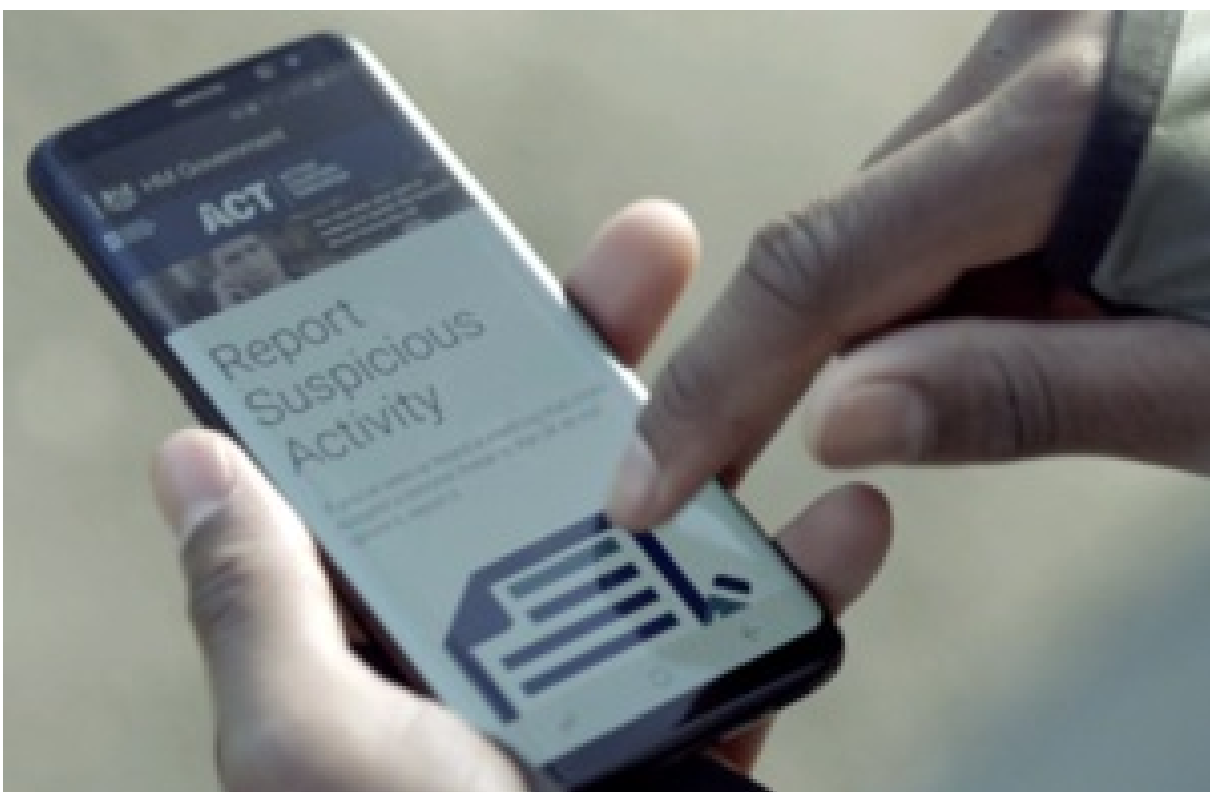
Crowded places include shopping centres, sports stadia, bars, pubs and clubs which are easily accessible to the public and attractive to terrorists.

This guidance has been written to help those charged with security at crowded places mitigate the threat and help make the UK less vulnerable to an attack.



## Action Counters Terrorism

Report suspicious activity and behaviour



NaCTSO urges the public to help the police tackle terrorism and save lives by reporting suspicious behaviour and activity.

Communities defeat terrorism. With the enduring terrorist threat, it is now more important than ever that everyone plays their part in tackling terrorism. Your actions could save lives.

Don't worry about wasting police time. No call or click will be ignored. What you tell the police is treated in the strictest confidence and is thoroughly researched by experienced officers before, and if, any police action is taken.

Any piece of information could be important, it is better to be safe and report. Remember, trust your instincts and ACT. Action Counters Terrorism.

## How can I report?

Reporting is quick and easy. You can report in confidence online via our secure form: [www.gov.uk/ACT](http://www.gov.uk/ACT). Alternatively, you can call the police confidentially on 0800 789 321. All reports are kept confidential and you can report anonymously. In an emergency always call 999.

## What should I report?

Like other criminals, terrorists need to plan. You can report suspicious activity or behaviour - anything that seems out of place, unusual or just doesn't seem to fit in with everyday life.



## What could potentially be terrorist-related suspicious activity or behaviour? Research

- Meetings, training and planning can take place anywhere. Do you know someone who travels but is vague about where they're going?
- Do you know someone with passports or other documents in different names, for no obvious reason?
- Do you know someone who looks at extremist material, including on the so-called Dark Web, or shares and creates content that promotes or glorifies terrorism?
- Have you noticed someone embracing or actively promoting hateful ideas or an extremist ideology?

## Gathering materials

- Suspicious materials can be ordered online as well as in store. Have you noticed someone receiving deliveries for unusual items bought online?
- If you work in commercial vehicle hire or sales, has a sale or rental seemed unusual?
- Have you noticed someone buying large or unusual quantities of chemicals, fertilisers or gas cylinders for no obvious reason?
- Have you noticed someone acquiring illegal firearms or other weapons or showing an interest in obtaining them?

## Storing materials

- Terrorists need to store equipment while preparing for an attack. Have you noticed anyone storing large amounts of chemicals, fertilisers or gas cylinders?



- Have you noticed anyone storing illegal firearms or objects that could potentially be weapons?

## Hostile Reconnaissance

- Observation and surveillance help terrorists plan attacks. Have you witnessed anyone taking pictures or notes of security arrangements or CCTV?

## Financing

- Cheque and credit card fraud are ways of generating cash. Have you noticed any suspicious or unusual bank transactions?

## What should I do if I find terrorist or violent extremist content online?



If you see online graphic or violent extremist material or content that supports, directs or glorifies terrorism please [report it using our anonymous online reporting form](#).

Terrorists use the internet to provoke individuals to carry out attacks in the UK.

One post or video has the power to influence vulnerable people and inspire extremists and terrorists. This is why it is important to tackle online terrorism.

You can help us stop terrorists' and extremists' online presence by reporting content such as

- Speeches or essays calling for racial or religious violence
- Videos of violence with messages in praise of terrorists
- Postings inciting people to commit acts of terrorism or violent extremism
- Messages intended to stir up hatred against any religious or ethnic group
- Bomb-making instructions
- Advice on how to obtain or make weapons

A specialist police team will examine the content and will work with the internet companies to remove it if appropriate.

---

## Hostile Vehicle Mitigation

Vehicle-borne threats range from vandalism to sophisticated or aggressive attack by determined criminals or terrorists. The mobility and payload capacity of a vehicle offers a convenient delivery mechanism for a large explosive device, although the vehicle itself may be used as a weapon. This section contains guidance that will help practitioners determine the vehicle-borne threat, assess site strengths and vulnerabilities, and identify suitable options for Hostile Vehicle Mitigation (HVM) measures.



## Determining the type of vehicle-borne threat being faced

When specifying the nature of the vehicle-borne threat it is important to understand:

- Modus Operandi (MO). This includes parked, penetrative, encroachment, deception and duress or a combination of attack methods including surreptitious and forcible attack on the barrier with hand tools or explosives
- Threat vehicle(s) - Unmodified road vehicles with specific characteristics - mass, speed and structure, as well as vehicle specific capabilities
- Blast effect - especially if considering VBIED attack
- Blast stand-off distance - must be considered in conjunction with the site operational needs and security plan

## How do I assess the strengths and vulnerabilities of my site to vehicle-borne threats?

Once the nature of threat is understood, practitioners should take a methodical and considered approach to determine project objectives and highlight security vulnerabilities:

- Develop detailed security requirements for HVM - Operational Requirements (OR)
- User Requirement Document (URD) if not covered in the detailed requirements - addressing additional business needs e.g. stakeholder liaison, planning and design
- Practical site assessment - a layered approach incorporating the local area, blast stand-off, traffic management and vehicle access control
- Technical assessment - e.g. Vehicle Dynamics Assessment (VDA) at specific locations based on the relevant threat vehicle(s)
- Liaison with technical or security experts - e.g. CPNI or CTSA advisers, or RSES professionals with relevant experience

## How can I reduce the vulnerability of my site and mitigate vehicle-borne threats?

Based on the project objectives and site assessment, a range of options can be incorporated into the design of a robust HVM strategy:

- Principles of hostile vehicle mitigation - determine the aims of the HVM strategy and how it will integrate with other site security measures
- Traffic calming - can be used to limit vehicle approach speeds to a manageable level
- Vehicle Security Barriers (VSB) - provide proven vehicle impact protection and maintain blast stand-off
- Traffic management - when and how legitimate traffic will access the site
- Vehicle access control - consider deployment of active VSB solutions, access procedures, long term operational management and emergency access

Remember if you see anything suspicious



Consortio Security is proud to host Project Griffin training for all employees and clients throughout the UK. The training is structured around a classroom environment and takes around 3 to 4 hours to complete. The training is delivered by Nathan Potter Consortio Security Chief Operating Officer.

### What is Project Griffin?

- Project Griffin aims to advise and familiarise Managers, Security Officers and Employees of public and private sector organisations across the UK on

security and counter-terrorism issues.

- It works by encouraging the public to be vigilant and to report suspicious behaviour and activity around their community. This will help to combat both terrorism and crime.
- Project Griffin was developed by the City of London Police and was introduced in central London in April 2004 as a joint venture between the City and Metropolitan police forces.
- Project Griffin has been adopted by Police Forces across the United Kingdom and overseas ever since.

Aims of Project Griffin:

- Project Griffin's aim is to engage, encourage and enable members of the community to work in partnership with the police to deter, detect and counter terrorist activity and crime.
- Project Griffin seeks to enlist the help and support of individuals or groups interested in maintaining the safety and security of buildings, businesses, areas or neighbourhoods.
- It provides an official and direct channel through which the police can share and update vital information relating to security and crime prevention.

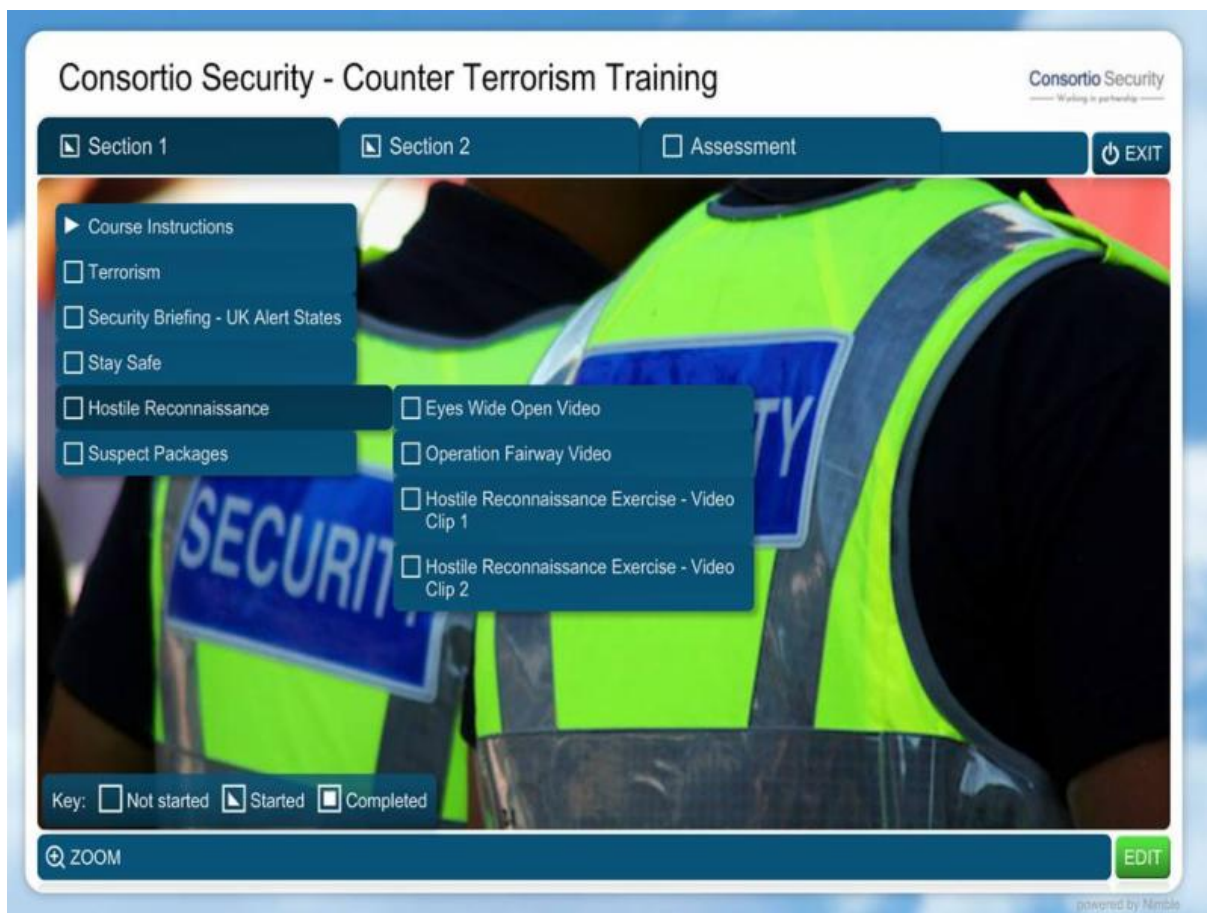
By

- Raising awareness of current terrorism issues.
- Giving people confidence to report suspicious activity to the Police.
- Sharing and gathering information.
- Building and maintaining effective working relationships.
- Seeking ways to combat terrorism and crime.
- Maintaining public trust and confidence in the Police and other authorities.

Should you wish to enrol on to this course or arrange a course in full at a location of your choice please feel free to contact Nathan Potter on 07932951651 or [N.Potter@consortiosecurity.com](mailto:N.Potter@consortiosecurity.com)

Or

Why not contact us, regarding our Counter Terrorism eLearning course



## Latest Safety, Security Alerts and Scams

### Cyber Smart



## SIMPLE STEPS TO PROTECT YOURSELF YOUR INFORMATION AND YOUR MONEY

### Keep up to date!

Whatever devices, operating systems, software or apps you use, always ensure you are running the most up to date versions. Updates include security patches to fix vulnerabilities! If you can, select 'Auto Update'.

### Antivirus

Make sure you have up to date antivirus installed and running for all devices you use to access the internet and email - make sure you are always running the most up to date. If you can, select 'Auto Update'.

### Passwords

You need to have a different password for everything you log in to. Make sure you're using #ThreeRandomWords to create a strong, separate password for each account.

### Protect your passwords

[www.haveibeenpwned.com](http://www.haveibeenpwned.com) - check to see if your details have been compromised. Click on the three lines and opt for notify me - you will be contacted anytime your passwords are found on the dark web allowing you to immediately change your passwords to protect accounts.

### BEWARE of phishing emails!

ALWAYS #TakeFive and REMEMBER! - emails, texts and phone calls can all easily be spoofed. NEVER assume any contact is genuine until you have verified that it is. Don't Click on links in emails or open attachments unless you are certain they are safe.

If an email relates to an account issue of any sort, always log in via a browser or an app - never click on a shortcut.

Did you know that you can forward suspected phishing emails to [NFIBPhishing@city-of-london.pnn.police.uk](mailto:NFIBPhishing@city-of-london.pnn.police.uk)

### iTunes Scams

NO legitimate debt can be paid in iTunes vouchers - #HangUp on that call

### Courier Fraud

Neither the Police nor Banks will ever contact you to:

- transfer money to a safe account;
- withdraw funds for safekeeping;
- assist with a covert investigation

OR

- collect cash, bank cards or PIN number

### Beware Free WiFi!

Fine for maps, bus timetables, weather etc - but do not risk sensitive information, such as being on social media, checking emails, banking, shopping etc - use your 3G or 4G on your phone.

Click on the below links for more Information

[Little Leaflet of Cyber Mistakes](#)

[Action Fraud Cyber Attack](#)

## Cyber Security



As the name suggests, the GCA Toolkit for Small Business is specifically designed for small and medium businesses to reduce the cyber risks they face on a daily basis.

The free online resource is available worldwide and offers actionable guidance and tools with clear directions to combat the increasing volume of cyberattacks.

The GCA Cybersecurity Toolkit arms small business owners with basic security controls and guidance, including:

Operational tools that help them take inventory of their cyber-related assets, create and maintain strong passwords, use multi-factor authentication, perform backups of critical data, prevent phishing and viruses, and more.

How-to materials, such as template policies and forms, training videos, and other foundation documents they can customize for their organizations.

### The Tools

- Know What You Have
- Update Your Defenses
- Beyond Simple Passwords

- Prevent Phishing and Viruses
- Protect Your Brand
- Defend Against Ransomware

The toolboxes and tools were carefully chosen based on the [Center for Internet Security Controls](#), the [UK National Cyber Security Centre's Cyber Essentials](#) and the [Australian Cyber Security Centre's Essential Eight](#)

About the Global Cyber Alliance (GCA): The GCA is an international, cross-sector effort dedicated to confronting cyber risk and improving our connected world. It is a catalyst to bring communities of interest and affiliations together in an environment that sparks innovation with concrete, measurable achievements.

## "Ask for Angela"

Police forces throughout the UK are working with venues to help prevent and reduce sexual violence and vulnerability.



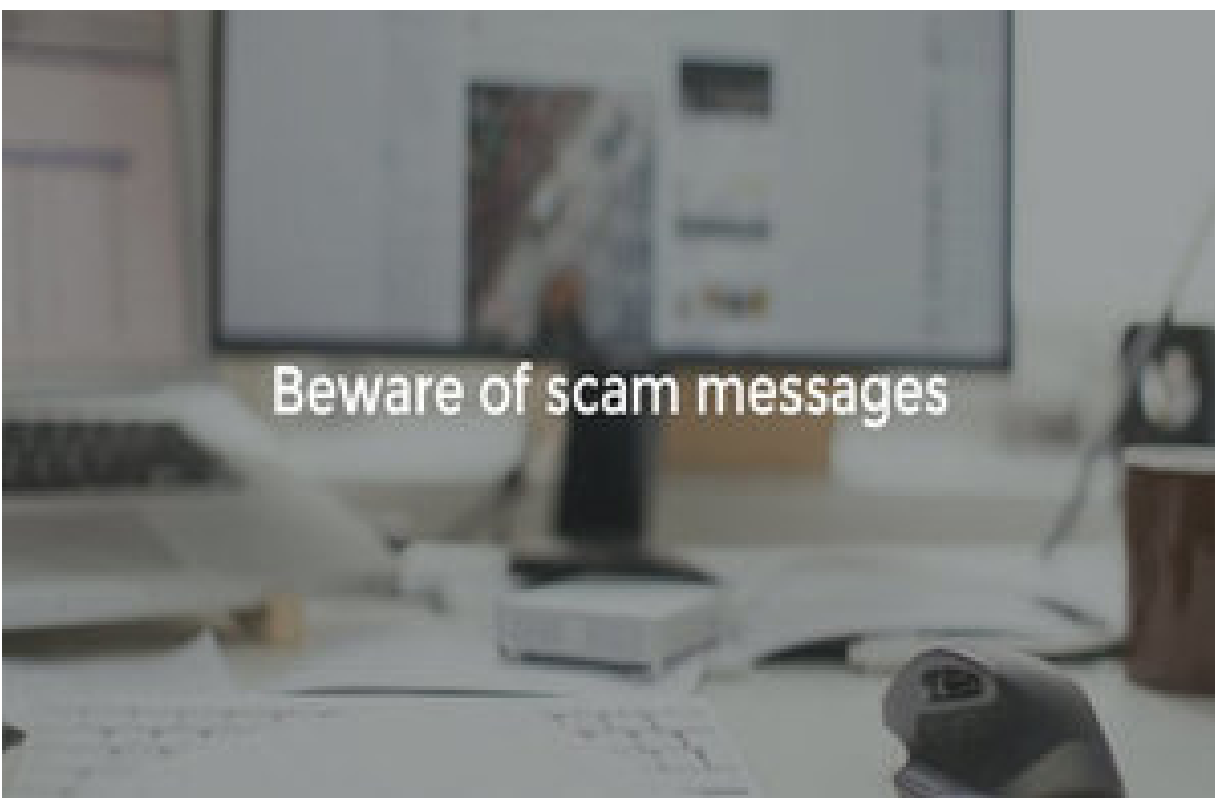
By telling customers that they can 'Ask for Angela' we're giving them a discreet codeword that they can give to staff if they feel unsafe or threatened.

The 'Ask for Angela' campaign is being reproduced with the permission of Lincolnshire County Council.

## Scam warning for DVLA customers

DVLA warns the public of scams asking you to provide your personal details and confirm credit card details.





We're aware that some members of the public are receiving emails, texts and telephone calls claiming to be from DVLA. Links to a website mocked up to look like a DVLA online service are sometimes included in the message. We don't send emails or text messages with links to websites asking you to confirm your personal details or payment information. We strongly advise anyone who receives such a request not to open the link and delete the item.

The government, led by Cabinet Office's Government Digital Service (GDS), will continue to investigate reports of organisations which may be actively misleading users about their services or acting illegally, taking swift action when necessary. By using the online [driving licence](#) or [vehicle tax](#) transactions on GOV.UK you can be sure that you are dealing directly with DVLA.