

Kent Fraud Alert System



TO STOP FRAUD™

Courier Fraud – Tunbridge Wells

Since my last series of alerts, we have seen continued attempts to target residents across Kent by criminal gangs for courier fraud but in particular those living in the Tunbridge Wells area. Please can you share this alert with family, friends, neighbours etc.

The criminals are still employing various methods from posing as Police Officers from multiple Kent Police Stations stating that they have arrested someone in possession of the victim's bank card to requesting financial information or asking victims to withdraw cash for a courier to collect as evidence.

If you get any calls like this, STOP, it is a scam.

The Police will NEVER ask you for financial details on the phone or request to collect your card or cash or gold as part of an investigation.

Remember the ABC of Scam Awareness and Never Assume or Believe a call is genuine and always Confirm.

If you get an expected call from someone claiming to be Police or any other organisation, then take their details and end the call. Then call back using a different phone if available. If another phone is not available, then wait 5 minutes and ring a family member or friend to ensure the line has been disconnected and then ring 101. Never call a number they have supplied and never ring 999 whilst still on the call with them. You must always disconnect the call first before ringing 101.

Watch - [Courier Fraud Warning: Stay Wise, Don't Compromise](#)



If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at [Advice about fraud | Kent Police](#)

You will also find valuable information from the Home Office at [Stop! Think Fraud - How to stay safe from scams](#)

Preventing fraud

Together,
let's stop
scammers.



Remember, ABC:



never Assume



never Believe



always Confirm



**Kent
Police**

Report a non-urgent crime online www.kent.police.uk/report

Talk to us on LiveChat – available 24/7 www.kent.police.uk/contact

In an emergency, if crime is in progress or life is in danger call **999**

If you have a hearing or speech impairment, use our textphone service **18000**.
Or text us on 999 if you've pre-registered with the emergency SMS service.

www.kent.police.uk   

Kent Fraud Alert System



TO STOP FRAUD™

Criminals Impersonating National Trading Stands (CTSI)

A Kent resident received a letter from CTSI claiming they are owed money from a wine company, with details of a court date. Thankfully, the resident did not respond and contacted the CTSI who confirmed this was not sent by them.

If you receive any letters like this, do not respond.

If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at [Advice about fraud | Kent Police](#)

You will also find valuable information from the Home Office at [Stop! Think Fraud - How to stay safe from scams](#)

Preventing fraud

Together,
let's stop
scammers.



Remember, ABC:



never Assume



never Believe



always Confirm



Kent Police

Report a non-urgent crime online www.kent.police.uk/report

Talk to us on LiveChat – available 24/7 www.kent.police.uk/contact

In an emergency, if crime is in progress or life is in danger call **999**

If you have a hearing or speech impairment, use our textphone service **18000**.
Or text us on 999 if you've pre-registered with the emergency SMS service.

www.kent.police.uk   

Kent Fraud Alert System



TO STOP FRAUD™

QR Code Scams in Kent make national news.

Over the last few months, I have been reporting/issuing alerts on scams involving QR codes being used by criminals in public places, in particular car parks.

Thanet, Ashford, Medway and Dover councils have recently been also issuing alerts with regards to this type of scam and this has now been reported by BBC News.

The QR stands for “Quick Response,” the black and white squares work like a two-dimensional barcode and can be scanned by a phone or tablet.

Businesses often use them to direct people to things such as app downloads, payment platforms, social media accounts, menus and events listings.

How to protect yourself -

- If you are not sure if the website a QR code takes you to is genuine, search for it in your browser instead.
- QR code scams can trick people into downloading malware - so ensure phone security is up to date.
- If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

To read this news item then go to - [Rise in reports of parking scams duping drivers in Kent - BBC News](#)



For further information about Fraud, visit our website at [Advice about fraud | Kent Police](#)

You will also find valuable information from the Home Office at [Stop! Think Fraud - How to stay safe from scams](#)



**Kent
Police**

Report a non-urgent crime online www.kent.police.uk/report

Talk to us on LiveChat – available 24/7 www.kent.police.uk/contact

In an emergency, if crime is in progress or life is in danger call **999**

If you have a hearing or speech impairment, use our textphone service **18000**.

Or text us on 999 if you've pre-registered with the emergency SMS service.

www.kent.police.uk   

Kent Fraud Alert System



Protect your online accounts from hackers and enable 2 step Verification

TO STOP FRAUD™

Action Fraud have issued a new warning about social media and email account hacking as new data is revealed.

This year Action Fraud and Meta are encouraging the public to protect their social media and email accounts as data shows there was a rise of social media and email account hacking reported in 2024, with a total of 35,434 reports made to Action Fraud, compared to 22,530 reports made in 2023. Action Fraud, the national fraud and cybercrime reporting service, has launched a campaign, supported by Meta, to encourage people to take an extra step of online protection by enabling 2-Step Verification (2SV) for each online account they have. The warning comes as reporting shows nearly £1 million was lost to hackers last year.

The most common motives for social media hacking were either investment fraud, ticket fraud or theft of the targeted account, reporting insights revealed.

In the reports made to Action Fraud, there were various methods of hacking highlighted, these include:

- **On-platform chain hacking** - This is when a fraudster gains control of an account and begins to impersonate the legitimate owner. The goal is to convince people to reveal authentication codes, including one-time passcodes, which are sent to them via text. Many victims of this type of hacking believe it is a friend messaging them, however the shared code was associated with their own account and the impersonator can now use it to access their account. Usually when an account is taken over, fraudsters monetise control of the account via the promotion of various fraudulent schemes, like fake tickets or crypto investment schemes, while impersonating the original account owner.
- **Leaked passwords and phishing** - The other common method of hacking is when account details are gained via phishing scams, or the use of leaked information used from data breaches, such as leaked passwords. This becomes prevalent as people often use the same password for multiple accounts, so a leaked password from one website can leave many of their online accounts vulnerable to hacking.

What can you do to avoid being a victim?

- **2-step verification (2SV) will keep criminals out of your account – even if they know your password.** Turning on 2SV gives your most important accounts an extra level of protection, especially your email and social media accounts. It can be turned on in a matter of minutes – time well spent to keep the fraudsters out. Find out how to enable it go to [Turn on 2-step verification \(2SV\) - Stop! Think Fraud](#)
- **Email and social media passwords should be strong and different to all your other passwords.** A good way to make sure your passwords are 'long enough and strong enough' is to combine three random words to create a unique password which is easy to remember. Find out more at [Improve your password security - Stop! Think Fraud](#)



**Kent
Police**

Report a non-urgent crime online www.kent.police.uk/report

Talk to us on LiveChat – available 24/7 www.kent.police.uk/contact

In an emergency, if crime is in progress or life is in danger call **999**

If you have a hearing or speech impairment, use our textphone service **18000**.

Or text us on 999 if you've pre-registered with the emergency SMS service.

www.kent.police.uk   

Kent Fraud Alert System



TO STOP FRAUD™

Fake Email Impersonating DVLA

I have received a message from a Kent resident about receiving a fake email from DVLA, informing them that DVLA could not collect their vehicle tax payment and that they needed to click on a link and update their payment details (see below).

If you get an email like this STOP, it is a SCAM. By clicking the link you are directed to a realistic website under the control of the criminals, where they will steal you financial and personal data.

DVLA will never send you an email like this.

If you think that you may have been a victim of this or any other type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at [Advice about fraud | Kent Police](#)

You will also find valuable information from the Home Office at [Stop! Think Fraud - How to stay safe from scams](#)

 GOV.UK

We hope this message finds you well. We are writing to inform you that your latest vehicle tax payment to the **Driver & Vehicle Licensing Agency (DVLA)** was unsuccessful.

To avoid any penalties or disruptions to your vehicle's tax status, we kindly ask you to update your payment details and complete the transaction as soon as possible.

[Update Now](#)

Our system will automatically retry the billing process once your billing details have been updated. It can take up to 5 working days for the records to update. To continue to the update page, please submit your vehicle tax details.

Please Note: If you don't pay your vehicle tax on time, you may be fined up to £1,000, or your details may be passed to a debt collection agency.

Preventing fraud

Together,
let's stop
scammers.



Remember, ABC:

 never Assume

 never Believe

 always Confirm



**Kent
Police**

Report a non-urgent crime online www.kent.police.uk/report

Talk to us on LiveChat – available 24/7 www.kent.police.uk/contact

In an emergency, if crime is in progress or life is in danger call **999**

If you have a hearing or speech impairment, use our textphone service **18000**.
Or text us on 999 if you've pre-registered with the emergency SMS service.

www.kent.police.uk   