

#### **Bogus Penalty Charge Text**

If you receive a text message like below, it is a SCAM.

You will notice the message does not provide any vehicle details, location, time or date when the alleged offence was supposed to have occurred.

If you click on the link, you will be taken to a realistic looking website under the control of the criminals, where they will steal your financial data.

You can report this by forwarding to 7726.



+ Text Message • RCS

.

### **Preventing fraud**



If you think that you may have been a victim of any type of scam, then contact your Bank immediately, which you can do by calling 159 and report it to Action Fraud at <u>www.actionfraud.police.uk</u> 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 <u>Stop! Think Fraud - How to stay safe from scams</u>



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.



# TO STOP FRAUD"

#### Quishing – How can I avoid becoming a victim?

I have reported on this scam regularly over the past year and a new alert has just been issued by Action Fraud, warning about this fraud type.

In the last year, £3.5M has been stolen nationally by criminals and it is on the increase.

Quishing is a form of phishing where a fraudulent QR code is scanned, designed to steal personal and financial information. The warning encourages people to stay vigilant and double check QR codes to see if they are malicious, or have been tampered with, before scanning them online or in public spaces. The most popular location for these has been car parks.

So, what can you do avoid being a victim of quishing?

- QR codes used in pubs or restaurants are usually safe to scan.
- Scanning QR codes in open spaces (like stations and car parks) might pose a greater risk. Check for signs that codes may have been tampered with (usually by a sticker placed over the legitimate QR code). If in doubt, do not scan them: use a search engine to find the official website or app for the organisation you need to make a payment to.

### **Preventing fraud**

Together, let's stop scammers.



Remember, ABC: <u>never</u> Assume <u>never</u> Believe <u>always</u> Confirm

- If you receive an email with a QR code in it, and you are asked to scan it, you should be cautious due to an increase in these types of quishing' attacks.
- Finally, we recommend that you use the QR-scanner that comes with your phone, rather than using an app downloaded from an app store.



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

For further information about Fraud, visit our website at <u>Advice about fraud | Kent Police</u>

You will also find valuable information from the Home Office at <u>Stop! Think Fraud - How to stay safe</u> <u>from scams</u>

ActionFraud



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.



#### Ticket fraud

Looking for last-minute tickets to this summer's top events? In 2024, over £9.7 million was lost to ticket fraud in the UK.

So, are you planning to buy tickets to go to this summer's hottest events?

Follow our tips to avoid ticket scams:

- Only buy tickets from official sources, direct from the venue's box office, the promoter, an official agent or a well-known and reputable ticket exchange site.
- Should you choose to buy tickets from an individual (for example on eBay or on a social media), avoid paying via bank transfer or virtual currency: never transfer the money directly into their bank account but use a secure payment site such as PayPal but never pay through the family/friends option.
- Paying for your tickets by credit card will offer increased protection over other payments methods, such as debit card, cash, or money transfer services. Avoid making payments through bank transfer or money transfer services, as the payment may not be recoverable.
- Check the contact details of the site you are buying the tickets from. There should be a landline phone number and a full postal address. Avoid using the site if there is only a PO box address and mobile phone number, as it could be difficult to contact customer services after you buy tickets. PO box addresses and mobile phone numbers are easy to change and difficult to trace.
- Before entering any payment details on a website, make sure the web address starts with https (the 's' stands for secure). There should be a locked padlock icon in the browser's address bar. Check if your ticket vendor is a @STARticketing member. Their members adhere to strict standards and offer an approved Alternative Dispute Resolution service.



If you think that you may have been a victim of any 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

TO STOP FRAUD

www.actionfraud.police.uk or call 0300 123 2040.

For further information about Fraud, visit our website at <u>Advice about fraud</u> <u>Kent Police</u>

You will also find valuable information from the Home Office at <u>Stop! Think</u> <u>Fraud - How to stay safe from scams</u>



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.





#### Fake Job Scams on Social Media

We are receiving reports in relation to fake job scams.

One resident on WhatsApp was looking for a job and was introduced to a criminal on WhatsApp claiming to own a care home agency. After talking about the job, the resident handed over £3,000 to pay for employment checks and was assured that if anything happened, they would get their money back. Unfortunately, no money was ever returned and there was no job or agency, it was a scam.

Personal information is extremely valuable to criminals. They use your details to impersonate you and apply for products and services such as bank accounts, loans, and credit cards. They may also target you asking for upfront fees.

- Spot the signs:
- Unrealistic salary
- Job offers without interview
- Poor written advert
- Being asked for money or personal details

For further information about this type of scam go to Employment fraud | Action Fraud



Together, let's stop scammers.



Remember, ABC:

<u>never</u> Assume

<u>never</u> Believe

<u>always</u> **C**onfirm



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

For further information about Fraud, visit our website at <u>Advice about fraud | Kent Police</u>

You will also find valuable information from the Home Office at <u>Stop! Think Fraud - How to</u> <u>stay safe from scams</u>



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.





#### **Courier fraud**

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.



and goods

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.

If you would like a copy of the leaflet opposite, please let me know by emailing stephen.kelly@kent.police.uk



as 'evidence'

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

cash, or bank

details

