

Kent Fraud Alert System



TO STOP FRAUD™

Quishing – What is it?



Quishing, also known as QR code phishing, represents a phishing technique that involves QR codes to trick potential victims. Like other types of phishing attacks, the purpose is to steal sensitive information, install malware on your device, or make you visit a website.

How Does Quishing Work?

Firstly, hackers plan a quishing attack by creating an innocent looking QR code. There are plenty of online tools to create a QR code, and you can even make a QR code on your Android phone.

QR codes can redirect you to false payment portals, malicious links, or host virus-infected documents. Hackers place malicious QR codes in places where victims are likely to scan them to achieve their goals. So QR codes placed on posters, flyers, and fake advertisements at public places might hide a phishing attack. This includes restaurants, malls, parks, and airports.

How can you 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.

Preventing fraud

Together,
let's stop
scammers.



Remember, ABC:

-  never Assume
-  never Believe
-  always Confirm

Get the latest
scam advice: 
@KentPoliceECU

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.



**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™

Black Friday

It is Black Friday and many of you maybe looking for online shopping bargains, both today and over the weekend.

Criminals are continually active at this time of year advertising too good to be true offers, either via fake websites or social media.

The following will take you to the relevant pages of the National Cyber Security Centre website with tips and advice on shopping safely online - [Shopping online securely - NCSC.GOV.UK](http://www.ncsc.gov.uk/shopping-online-securely)

Remember to conduct your research and trust your instincts and if you think something is not right, then do not buy and instead report it.

You can report a scam website to [Report a suspicious website - NCSC.GOV.UK](http://www.ncsc.gov.uk/report-a-suspicious-website)

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.

Preventing fraud

Together, let's stop scammers.



Remember, ABC:

-  never Assume
-  never Believe
-  always Confirm

Get the latest scam advice:



@KentPoliceECU

BE BLACK FRIDAY SAVVY NOT EVERYTHING YOU SEE IS REAL

Taking a moment to stop and think before parting with your money or information could keep you safe. Be suspicious of any "too good to be true" offers or prices. Question purchases that require you to pay by bank transfer instead of using the online platform's secure payment options.

Could it be fake? If you believe you've fallen for a scam, contact your bank immediately on a number that you know to be correct and report it to Action 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



Fake DVLA Text Messages

Following on from our alert last week of a rise in fake DVLA emails, we are now being made aware of fake text messages impersonating DVLA. The message may be in various forms but one of the most popular is that your payment has been missed and you need to click on a link and update your Bank details. If you click the link, you will be directed to a convincing looking website under the control of the criminals, where they will steal your financial and personal data.

DVLA will never text and ask you to update payment details. If you get a text like this, you can report it by forwarding to 7726.

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 STOP FRAUD™

Preventing fraud

Together,
let's stop
scammers.



Remember, ABC:

 never Assume

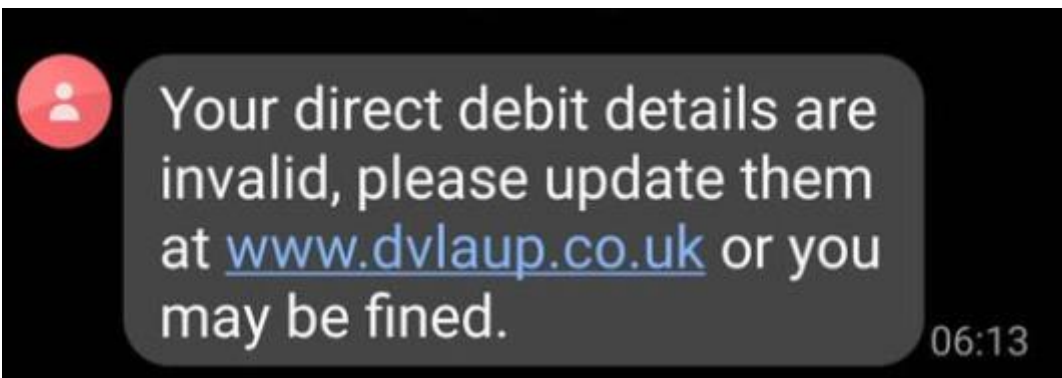
 never Believe

 always Confirm

Get the latest
scam advice:



@KentPoliceECU



**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™

Black Friday Fake emails

Action Fraud has received 2,035 reports about Black Friday scam emails.

The emails will ask you to click on a link which will direct you to a convincing looking website, where the criminals will steal your personal and financial data.

You can report suspicious emails by forwarding to - report@phishing.gov.uk

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.

Preventing fraud

Together, let's stop scammers.



Remember, ABC:

 never Assume

 never Believe

 always Confirm

Get the latest scam advice: 

@KentPoliceECU

Black Friday scam emails

Action Fraud has received over 2,000 reports relating to fake emails about Black Friday offers and deals. The emails usually purport to be from well-known brands and retailers, claiming to offer special offers and deals for Black Friday. The links in the email lead to fake websites designed to steal your personal and financial information.

If you have doubts about a message, contact the organisation directly. **Don't** use the numbers or address in the message - use the details from their official website. Your bank (or any other official source) will never ask you to supply personal information via email.

Spotted a suspicious email? Forward it to the Suspicious Email Reporting Service (SERS) - report@phishing.gov.uk



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™

Courier Fraud Alert

We have received reports this week, particularly in the Maidstone area with criminals impersonating Police. In several of the attempts they have stated that they are an officer from Guildford Police station. They will say that someone has been arrested with your bank card or ask you to assist with an investigation by withdrawing cash from your bank for them to collect.

Please remember, the Police will NEVER send a courier to your address to collect your CARD's and PIN numbers or CASH as part of an investigation.

If you get a call like this, then hang up.

If uncertain, then take their details and hang up and ring 101 using a different phone. If you do not have another phone, then wait 5 minutes and ring a family member or friend to confirm that the line has been disconnected and then ring the Police.

Never ring back using a number that they have supplied.

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.

Preventing fraud

Together,
let's stop
scammers.



Remember, ABC:

 never Assume

 never Believe

 always Confirm

Get the latest
scam advice:



@KentPoliceECU

COURIER FRAUD ALERT!



**TARGETING RESIDENTS IN WEST
KENT, MAIDSTONE, ROCHESTER
AND SITTINGBOURNE**



**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   