

Kent Fraud Alert System



TO STOP FRAUD™

Calls impersonating Medway Council

Medway Council have issued the following alert in relation to a member of the public having received a call from a number that was spoofing a Medway Council number.

“Residents are being warned about potential scam calls from a false Medway Council phone number.

In a recent case reported on Monday, July 29, a householder received two calls in which a recorded message stated there had been unexplained activity on their bank account – which proved to be incorrect.

The calls are believed to be made using a “spoof” number, which is when scammers change their caller ID to disguise their identity from the person they are calling.

To avoid risk of fraud, never give out personal information in response to a call or rely upon the Caller ID as the sole means of identification, particularly if the caller asks you to do something which might have financial consequences. If someone rings you asking for your bank details, do not provide them.”

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.

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



**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™

Nat-West Fake/Phishing Emails

Be on the lookout out for these FAKE NatWest emails claiming that your account's contact number has been updated.

Action Fraud have reported receiving over 151 reports of these across the UK. The email will state that your request to change your mobile number on your account has been received and updated but that if it was not you requesting the update, then click on the link within the message to cancel the request.

However, it is a scam and the link will take you to a realistic looking website under the control of the criminals where they will steal your personal and financial data.

If you receive a communication from your Bank and are uncertain, you can contact them by ringing 159.

Preventing fraud

Together,
let's stop
scammers.



Remember, ABC:

 never Assume

 never Believe

 always Confirm

Get the latest
scam advice: 

@KentPoliceECU

NatWest scam emails

Action Fraud has received over 151 reports in two weeks relating to fake emails purporting to be from NatWest. The emails claim that the contact number on the recipient's bank account has changed. The links in the emails lead to malicious websites that are designed to steal personal and financial information.

HOW TO DEAL WITH SUSPICIOUS MESSAGES

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



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



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™

How to Report various Fraud Types

If you are a victim of fraud or an online crime (cybercrime) you can report to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

Additionally, you can report other types of Fraud and Scams to the following,

- [business or personal tax fraud to HMRC](#) (Her Majesty's Revenue and Customs)
- [scams to do with HMRC directly to them](#)
- [benefit fraud on GOV.UK](#)
- [immigration fraud to the Home Office](#)
- [counterfeit \(fake\) medicine or medical devices to the Medicines and Healthcare products Regulatory Agency \(MHRA\)](#)
- [online child abuse or suspicious online behaviour involving a child to your local police force or to the Child Exploitation Online Protection Command](#)
- [Report fraud, bribery or corruption | Kent Police](#)
- [Electoral fraud | Kent Police](#)

You can report fake/phishing emails by forwarding to Report@phishing.gov.uk and fake text messages by forwarding to 7726 (Spam).



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™

Fake Evri Text messages

A Kent resident asked that I remind everyone about the threat of fake text messages impersonating Evri, as they received a text from a mobile number about re-delivering a parcel. As the intended victim was expecting a parcel, they unfortunately clicked on the link within the text message and started to complete their details. However, when it started to ask for personal data, they realised it was scam. Then applying the scam awareness of ABC (never Assume or Believe a message is genuine and always Confirm) they contacted the company who confirmed it was scam.



Information on Evri's website states the following –

“How will Evri contact you?”

Generally, we will contact you by email or text message to advise where your parcel is in our delivery process. At times, this may include a tracking link. We may also contact customers by email or text message and ask for information in relation to an ongoing claim.

- Our emails will typically be from @evri.com, @hermes-europe.co.uk or @myhermes.co.uk.

Our SMS messages:

- Will not show the sender's name as a mobile phone number.
- Will never ask you for payment.
- Will never include a link except for a tracking link called <https://evri.link/.....> (Please be aware even if the link does show as <https://evri.link/.....> we cannot guarantee this is genuine. If you are unsure do not click a link and do not enter any personal details.

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 www.kent.police.uk | [Advice about fraud | Kent Police](http://www.kent.police.uk)

Preventing fraud

Together, let's stop scammers.



Remember, ABC:



never **A**ssume



never **B**elieve



always **C**onfirm

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™

Amazon Scams

Whilst travelling around the county delivering presentations to various groups, several people have stated there is a high level of fake Amazon phone scams and text messages circulating. Therefore, I thought it would be useful if I circulated the official information from Amazon on how to identify if a call or text message is fake. Please see the following -

“How do I know if a call was from Amazon?”

If you receive a suspicious phone call claiming to be from Amazon, here are some things you can look out for:

- Amazon will never ask for payment or offer you a refund you do not expect.
- Amazon will never ask you to make a payment outside of our website (EG via bank transfer, e-mailing credit card details, sharing gift card details over the phone, etc.)
- Amazon will never ask you for remote access to your device EG by asking you to install an app.”



In relation to fake text messages, they state the following –

“How do I know if an SMS was from Amazon?”

Smishing scams are becoming increasingly advanced: Scam messages can be inserted into a thread of legitimate messages that you might have received from Amazon. If you receive a suspicious SMS claiming to be from Amazon (sometimes called Smishing), here are some things you can look out for:

- Scam texts will often say there is a problem with your account, ask you for sensitive information like passwords, or state that you are owed a refund. Amazon will never ask for your password or personal information by text Message.
- Amazon will never ask for your personal information, or ask you to make a payment outside of our website (EG via bank transfer, e-mailing credit card details, etc.) and will never ask for remote access to your device EG by asking you to install an app.”

Preventing fraud

Together, let's stop scammers.



Remember, ABC:

-  **never Assume**
-  **never Believe**
-  **always Confirm**

Get the latest scam advice:  [@KentPoliceECU](https://twitter.com/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   