

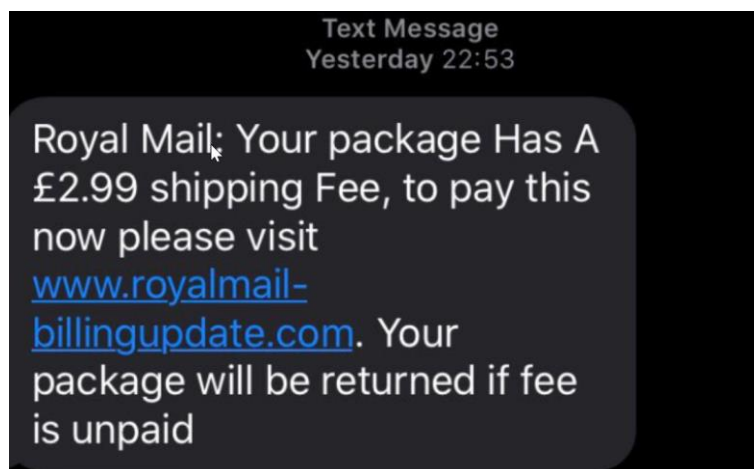
Kent Fraud Alert System



TO STOP FRAUD™

Post Office Text Scam

If you get Text like this –



It is a scam!!! The link takes you to a website operated by Fraudsters who are looking to steal your banking information and drain your hard earned monies from your bank accounts or take out loans/overdrafts etc. using your personal data.

Royal Mail will never send a text message of this kind or ask you to click on a link. If you get a text message like this then please forward the text to 7726 (SPAM, who will then look to take it from there.

If you believe you have been a victim of this scam, then contact your bank, immediately and report it to Action Fraud at www.actionfraud.police.uk or by calling 0300 123 2040.

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)



**Kent
Police**

Contacting 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 deaf or speech impaired, text '**police**' and your message to **60066**

www.kent.police.uk   

Kent Fraud Alert System



TO STOP FRAUD™

Hoax Alert

I have had a few emails this week asking about the below message appearing on social media.

BE VIGILANT. Straight from the City of London Police fraud team - Extremely sophisticated scam going about this week, involving all banks. You get a message saying a payment hasn't been taken e.g O2, Vodafone, 3, Giff Gaff or EE and to click here. As soon as you touch it your money is gone. They already have all your details and it's the most advance scam the bank has ever seen. Pass this on to everyone please. This is straight from work this morning - the banks are being inundated with calls - thousands flying out of peoples accounts! Spread the word to your family and friends!" Be vigilant !!!!

This is a hoax message that surfaces from time to time. If you see this, please disregard, as it is not a genuine message.

However, phishing scams are a real problem and you should never give out personal details, such as passwords or pins, over the phone. If you believe you have shared personal details with a fraudster, immediately contact your bank. Remain vigilant and use the ABC of Fraud Awareness.

Preventing fraud

Together,
let's stop
scammers.



Remember, ABC:



never Assume



never Believe



always Confirm

Get the latest
scam advice:



@KentPoliceECU



**Kent
Police**

Contacting 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 deaf or speech impaired, text '**police**' and your message to **60066**

www.kent.police.uk



Kent Fraud Alert System



TO STOP FRAUD™

What is Sim Swap Fraud?

When a fraudster tricks your network into transferring your mobile number to a new Sim card in their possession meaning they receive all calls and texts intended for you, including any one-time security passcodes required to access your accounts.

There are a number of ways criminals obtain your data, E.G. either through social media, paying for stolen data or through social engineering (fake emails, texts or phone calls that trick you into giving out your details). With this information they then pose as you in order to contact your network provider and request that your number is switched to a new Sim card that they have. They are then able to access your social media, email and Bank Accounts.

What can I do to protect myself

- Add a password or passcode to your mobile account
- Restrict who can see your social media profiles which can often contain information that is then used in security questions (i.e. name of first school, date of birth, children's names etc)
- Remember to be vigilant if you get calls, texts or emails asking for information. Remember ABC – Never Assume or Believe they are genuine and Always Confirm that they are.
- Call your provider immediately if you receive unexpected texts or emails about 'porting your Sim' or a PAC request, or if you suddenly lose phone signal.
- If your Sim has been swapped, alert your bank immediately in case the fraudster tried to make a transfer from your account.
- Check with your mobile or landline provider about what additional security they can put in place to prevent your number being diverted without your permission.
- If your mobile phone service stops unexpectedly, notify your bank.



**Kent
Police**

Contacting 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 deaf or speech impaired, text '**police**' and your message to **60066**

www.kent.police.uk



Kent Fraud Alert System



TO STOP FRAUD™

Text Messages impersonating your Bank

If you get a text message from your bank like this, it is a scam!!!

LLOYDS: A payment was attempted from a NEW DEVICE on 18/03 at 19:50:23 and needs approval. If this was NOT you, please visit [https://\[redacted\]](https://[redacted])

Barclays Alert: You have successfully added a new pay 18/02/2021 at 20:27. If this was you cancel via: [https://\[redacted\]](https://[redacted])

HALIFAX: You have successfully added a new payee Mr M KH/ ending in 3994, if this was not please visit: [https://\[redacted\]](https://[redacted]) to secure your account

HSBC: A payment was attempted from a NEW DEVICE on 23/03 at 12:13PM. If this NOT you, please visit: [https://\[redacted\]](https://[redacted])

Messages like this impersonating/spoofing a number of banks and financial institutions are currently being sent by fraudsters to innocent victims, in order to get you to click on a link and obtain your banking data. If you get one of these, do not click the link but instead forward the text to 7726 (Spam). If unsure, then contact your Bank using a trusted number which can normally be found on the back of your debit/credit card.

If you believe you have been a victim of this scam, then contact your bank, immediately and report it to Action Fraud at www.actionfraud.police.uk or by calling 0300 123 2040.

Preventing fraud

Together, let's stop scammers.



Remember, ABC:



never Assume



never Believe



always Confirm

Get the latest scam advice:



@KentPoliceECU



**Kent
Police**

Contacting 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 deaf or speech impaired, text 'police' and your message to **60066**

www.kent.police.uk

