Sim Swapping is becoming more common but what is it?

Sim swap fraud happens when criminals transfer your phone number to their SIM card. This gives them control of your phone number, so they can receive your calls and texts. Fraudsters can then use two-factor authentication (2FA) to change your passwords and access emails and accounts.

Follow these tips to stay safe.

- **Protect your personal information:** never share valuable information like your bank account details or passwords. Ignore unexpected requests for your details.
- Set up a PIN or password with your phone provider: ask your provider to set up a unique PIN or password on your account, needed to approve any account changes.
- Use social media wisely: avoid sharing details such as your phone number, date of birth and answers to common security questions.
- Monitor your accounts: regularly check your bank accounts and credit reports for strange transactions or activities. Set up alerts for any significant changes to your accounts.
- Check with your Bank about setting up biometrics: this will add an extra level of security to your account.

How to spot SIM swapping

Contact your phone provider and bank if you spot any of these signs.

- **Sudden loss of service:** if your phone suddenly loses service and you cannot make or receive calls or texts, it could be a sign that a criminal moved your number to another SIM card.
- **Notifications of suspicious activity:** if you receive log in or SIM activation notifications which was not you, it could be a sign that criminals are trying to move your number to a new SIM.
- Loss of access to your accounts: if you cannot access your email, bank, or social media accounts, it could be a sign that a criminal has taken control of it.
- **Unauthorised transactions:** if you spot payments on your account that you do not remember making, it could be a sign that a criminal has accessed your account.

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> and 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.

www.kent.police.uk





Together,
let's stop
scammers.Image: ConfirmRemember, ABC:
Image: never AssumeImage: never assume
Image: never assume





Emergency Alert UK date set.

The test Emergency Alert will take place at approximately 15.00 on the 7th of September 2025. Why is the Emergency Alert test taking place?

Emergency alerts are used by many countries around the world. They function as an effective way to warn people when there is a danger to life nearby, for example extreme weather conditions.

Ahead of the upcoming test, the Cabinet Office says it will be running a public information campaign to inform people about the test.

However, this may also provide an opportunity for criminals, so remember, no one will be contacting you requesting that you supply personal data, account details etc. or sending texts and emails asking you click on links.

Always be wary of links in messages.



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 0300 123 2040.

For further information about Fraud, visit our website at <u>Advice about fraud | Kent Police</u> and you will also find valuable information from the

Home Office at <u>Stop! Think Fraud - How to stay</u> safe from scams



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



Preventing fraud

Together, let's stop scammers.



Remember, ABC:

🦳 <u>never</u> Assume

<u>never</u> Believe

🕛 <u>always</u> **C**onfirm

Impersonation Scams

Major high street retailers have recently experienced cyber-attacks. Be extra cautious with emails or messages claiming to be from these stores. Fraudsters often use current news stories to lure you in, impersonating trusted brands to conduct phishing scams aimed at stealing your personal information.

If you receive an email that you are not sure about, take these steps:

- Look at the sender's email address scam emails are typically sent • from random addresses comprised of a mix of numbers and letters. Brands might have their official email addresses listed on their websites, so make sure to check these out. You can find the sender's email address by hovering your cursor over or right-clicking on the sender's name.
- See if the greeting is impersonal, as most brands will address you by • name.
- Look out for blurry, pixelated and out-of-date branding. Beware of pressure tactics, such as a short deadline, to claim an offer.
- Check the links in the email by hovering over where you would expect to see one, such as where it says, 'click here,' to see where the message leads.
- Be suspicious of emails asking for your personal or financial details. •
- Watch out for poor spelling and grammar. •
- Always be wary of messages asking you to click on a link, as these will take you to a website that ٠ maybe under the control of criminals.

If you receive an email from a brand, you have an account with and you are not sure whether it's genuine, you should log in to your account using a website you've used before and know can be trusted or, you can use a website that you are independently searched for on a search engine. Once you have logged in, you should verify the information in the email before following any links from the email. You could also call the customer service number using details from its official website or a recent letter.

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 0300 123 2040.

For further information about Fraud, visit our website at Advice about fraud | Kent Police and you will also find valuable information from the Home Office at Stop! Think Fraud - How to stay safe from scams



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





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

TO STOP FRAUD

Preventing fraud

Pet's Corner and associated Scams

Criminals are always looking for ways to scam you out of your hard earned cash and are always looking for ways to take advantage of the current cost of living crisis. Anyone who is a pet owner, knows the costs of vet's bills.

Recently, an urgent warning has been issued to pet owners by the UK Government after an owner unknowingly purchased a counterfeit flea treatment online that caused the cat to become seriously ill. This prompted the owner to get the product tested and toxic pesticide traces were found. See here for the full story <u>Urgent warning to pet owners as toxic chemicals found in fake</u> <u>flea treatments - GOV.UK</u>

Shopping safely for pet treatments -

- Always buy flea treatments from trusted sources
- Be wary of any retailer selling prescription only products without asking for your prescription. This is illegal.
- If a deal or offer looks too good to be true, it probably is! If you need advice, contact Citizens Advice on 0808 223 1133.



Preventing fraud

Together, let's stop scammers.



Remember, ABC: <u>inever</u> Assume <u>inever</u> Believe <u>inever</u> Confirm

Please stay alert and "Bubbles" (see picture below) says please share this with family and friends, especially those who might be more vulnerable to these types of scams and help protect my animal friends.



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> and you will also find valuable information from the

Home Office at <u>Stop! Think Fraud - How to stay safe</u> from scams



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





Crypto Currency Scams

We have recently received several reports of cryptocurrency scams. Do you know how to spot the signs of a fraudulent investment?

Investment scams are becoming increasingly difficult to identify but there are some telltale signs that can help protect your hard-earned money:

- Do not be rushed into making an investment.
- Seek independent financial advice first, e.g., from your bank.
- Check if the company is registered with the FCA.

Learn more at ScamSmart - Avoid investment and pension scams | FCA

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 |</u> <u>Kent Police</u> and 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:

<u>never</u> Assume

<u>never</u> Believe

🕛 <u>always</u> **C**onfirm

DON'T BE FOOLED

Victims of cryptocurrency fraud report being lured in by glossy websites, social media posts and online ads.



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.

www.kent.police.uk

