

Keep Your Money Safe



Surrey Police and Sussex Police Fraud Newsletter

In this issue:

Mobile phone delivery scam warning

Report Fraud Social Media and Email Hacking Webinar

Bank impersonation fraud

MOBILE PHONE DELIVERY SCAM WARNING

Surrey Police and Sussex Police are reminding residents to be wary of a scam currently circulating where criminals use stolen personal information to order mobile phones in their own or someone else's name. We have received several reports from residents in both forces being contacted by fraudsters claiming to be from companies including Sky and Three.

Stolen details are used to take out or access a mobile phone account and arrange for a handset to be delivered to the victim's address. Soon after the phone arrives, the victim may receive a call, email or message from someone claiming to be from the mobile network, retailer or delivery company. They will often say the phone was sent in error and ask for it to be returned or handed over to a courier.

Unfortunately, if the phone is passed on without checking the request is genuine, the criminals walk away with the handset, and the victim could be left dealing with the consequences of a fraudulent account opened in their name.

If a mobile phone is delivered to your address that you did not order, do not hand it over to anyone until you have confirmed the situation directly with the supplier. Always use contact details from the company's official website and be cautious of phone numbers, emails, messages or collection arrangements provided by someone who contacts you unexpectedly.

“Each month we see many incidents of fraudsters targeting our residents in an attempt to defraud them. We're working hard to prevent this and support vulnerable victims of fraud or scams. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim.”

Detective Chief Inspector
Antony Leadbeatter
Surrey Police &
Sussex Police
Economic Crime Unit

Adding extra security to your mobile account, such as a PIN, password or memorable word, can help prevent unauthorised access. It is also good practice to regularly check your bank and mobile phone accounts for anything unusual. Services such as <https://www.cifas.org.uk/> can also help you monitor for signs of identity fraud.

Remember, if an unexpected phone is delivered to your address, take the time to verify who it belongs to before agreeing to any collection or return. If anyone attends your address and you feel threatened or unsafe, call 999 immediately.

Join the Report Fraud Social Media and Email Hacking Webinar

As part of Cybersecurity Awareness Month, Report Fraud is hosting a webinar on protecting your email and social media accounts from hackers and fraudsters.

The session will cover the latest threats, practical security measures, and the simple steps you can take to keep your accounts safe from compromise. Whether you're looking to strengthen your own online security or help protect friends and family, this webinar will provide expert guidance and actionable advice.

Register your place here:

<https://events.teams.microsoft.com/event/53994f64-090f-4887-8744-3422da79ad56@9386af3d-781b-4bad-8559-7170be76bad9>

£6.3m was stolen
through email and
social media account
hacking in 2025/26



Bank impersonation fraud

This complex fraud begins with a simple text message....

Surrey Police and Sussex Police have seen a sudden and sharp increase in bank impersonation scams, starting with a text message.

One report said the victim received a text message saying there was fraudulent activity on her bank account and to click the link to prevent the transaction. Having clicked the link, she was contacted on WhatsApp from someone claiming to be from the Barclays fraud team. Using lengthy and convincing tactics, to obtain security information and access her devices, the fraudster eventually stole £5000 from her accounts.

Another example saw a text message from 'Barclays' advising a fraudulent payment had been detected. The victim was instructed to "reply Y to the text to attempt the payment again if this was you, and if not recognised call this number", which he subsequently did. Again the conversation was lengthy and complex and sadly resulted in the loss of hundreds of pounds.

Your bank will never say your money is at risk and that you need to move it. If anyone says this, it's a scam – don't follow their instructions.

The contact may appear convincing by using official-looking phone numbers, logos or even the names of genuine employees. They will usually claim there is a problem with your account, suspicious activity, or an urgent security issue that needs immediate action.

Their aim is to create a sense of panic so that you act quickly without stopping to think. Victims may be persuaded to transfer money to a so-called "safe account", withdraw cash, or share personal and banking information. In reality, the money or information is being handed directly to criminals.

If anyone contacts you unexpectedly and asks you to send them money, don't do it. Instead, call them on a number you know is genuine to check the request is real. If it's a company, get their number from their official website.

If something doesn't feel right, hang up, wait a few minutes, and contact the organisation directly. Trust your instincts and don't let anyone pressure you into making rushed decisions.