

WELCOME TO THE BIG CON

PROTECTING YOU FROM SCAMS, ONE ISSUE AT A TIME

**Stop!
Think
Fraud.**

**Did you
know?**

Dial 159

If a call claiming to be from your bank feels off, hang up and dial 159.

159 is a shortcode that connects directly to your bank's fraud department.

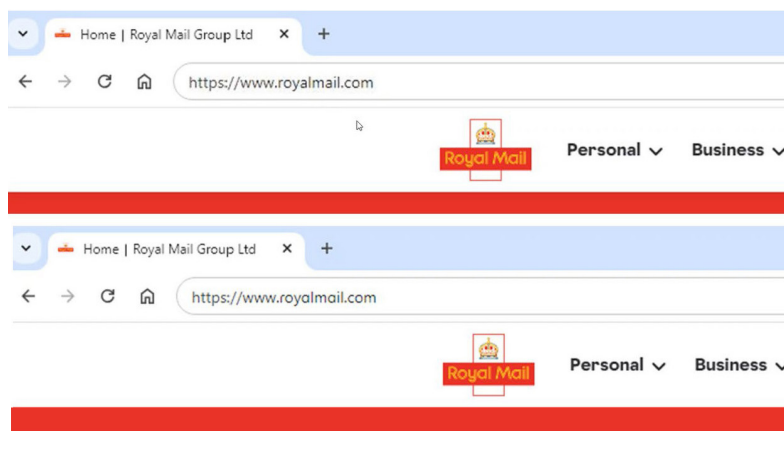
It covers 99% of all UK Bank's

No searching, no fake numbers. 159 cannot be spoofed and guarantees a safe route to your bank.

Calling from a landline? Wait five minutes before dialling.

The Big Con

Test your knowledge, can you spot the fake:



Fraud is everywhere—and it's constantly evolving.

The Big Con is here to help you stay one step ahead with clear advice, real world examples, and simple habits that make a big difference.

From convincing calls, texts, and emails to emerging fraud

tactics, each issue will break down real scams so you know what to spot, what to avoid, and how to protect yourself. A little knowledge goes a long way—small changes can make a big difference.

**Get
involved
ask us
anything**

Seen a scam or unsure if something's legitimate? Send it in via the email listed below. The Fraud Team is here to help.

**Share
your story**

Spotted a scam, or been caught by one? Your experience could help protect others in a future issue.

Stay safe

**Pause before
you click or
respond.**

An organisation won't pressure you to act immediately. Stop! Think Fraud.

Trust your instincts.

**Stop!
Think
Fraud.**

Phishing explained

Phishing is a scam where criminals 'fish' for your information by pretending to be trusted organisations—such as banks, delivery companies, or government bodies. These messages can arrive by text, email, social media, or phone and are designed to make you act quickly.

Why it works

Phishing is fast and effective. Scammers send thousands of messages at once—and just one click is enough.

Watch for the red flags such as:

- Unexpected requests to confirm details
- Messages creating urgency or alarm

- Spelling mistakes or odd formatting
- Requests for personal information, passwords, PINs, or onetime codes

Stay Safe

- Be cautious with unexpected messages
- Check sender details carefully
- Never share personal or security information

- Avoid links - go straight to official websites or apps
- Let unknown or withheld calls go to voicemail

Report and delete

Forward texts to 7726, send emails to: report@phishing.gov.uk

Always assume it's a scam until proven otherwise.

Send your story for a future issue: TheBigCon@derbyshire.police.uk

Case study: When a 'bank alert' wasn't the bank

After spotting suspicious activity, a customer did the right thing—contacting their bank, which cancelled the card and confirmed the issue was under control.

Three days later, a convincing text arrived in the same message thread as genuine bank alerts. It warned of a £330 eBay purchase and asked for a reply if it wasn't recognised. Trusting the format, the customer responded.

Minutes later, a call followed. The caller claimed to be a senior bank investigator, using professional language and referencing the earlier fraud report. He warned that "corrupt staff" were putting the customer's savings at risk and urged

immediate action.

Under pressure, the customer was persuaded to move money to a "safe account" and even open a new one. Over the next two days, constant calls kept the customer anxious and compliant. Multiple payments were made—and a £25,000 loan was taken out in their name without their knowledge.

Key red flags

- Unexpected bank text
- Urgent pressure to act
- Claims of internal bank corruption
- Requests to move money or open a new account
- Ongoing manipulation through repeated contact

Always assume it's a scam until proven otherwise. A busy day, a rushed click. That's all they need.

Myth vs Fact

Myth: Fraud only happens to the vulnerable

Fact: Fraud can strike anyone. In the UK, 88% of young people aged 13–21 reported encountering suspected fraudulent content online in the past year. Nearly one in three (29%) had been a victim of fraud. (Source:science.

police.uk). This shows that age and digital confidence don't offer protection.

Fraudsters aren't looking for "easy targets". They look for moments of weakness: a busy day, a rushed click. That's all they need.

Community support

We offer free, interactive scam awareness sessions for community groups. Get in touch to arrange a visit.



Editor's note: This newsletter has been written by officers and staff from Derbyshire Constabulary to highlight the signs of fraud and how to protect against it. This inbox is not monitored 24/7, so please do not report crime to this email.

If you've got any feedback, or stories you'd like to be included in future editions please email TheBigCon@derbyshire.police.uk.

12:09

77%

< 213



+44 7709 232... >

Text Message • SMS
Wed 21 Jan at 17:33

NatWest:
Transaction attempt to
EBAY amounting to
£330.99 is currently on
hold pending a payment
review. If this was NOT
made by you reply (N)
now.

N

If you did not expect this message from an unknown sender, it may be spam.

[Report Spam](#)

Text Message • SMS



The takeaway

This scam worked because it felt real, urgent, and personal.

Remember:

Your bank will never ask you to move money to keep it safe. If something feels off—stop, hang up, and contact your bank using trusted details.