

BANK

ISSUE 66

SCAMS AWARENESS
NEWSLETTER

MAY 2026

WELCOME TO OUR

Monthly Newsletter

Don't move your money – spotting bank impersonation scams



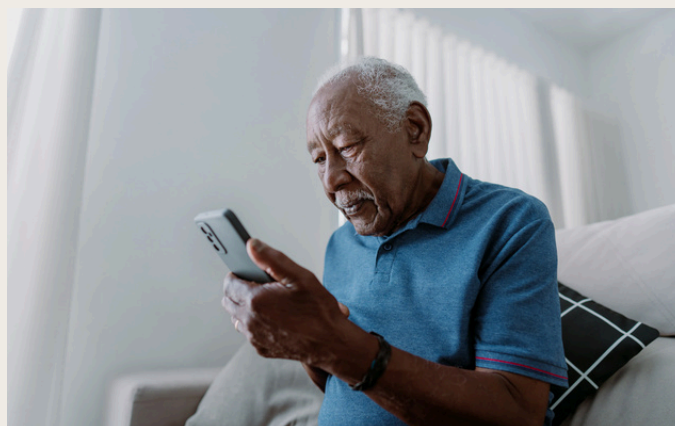
F R A U D

In this newsletter:

- Bank impersonations and how they work p.2
- How to protect yourself and staying safe p.3
- What to do and a three-step rule p.4

Bank impersonation scams remain one of the most convincing and damaging types of fraud affecting people across the UK today. These scams are highly organised, carefully planned, and often involve criminals who sound professional, calm, and reassuring. Unfortunately, this makes them very difficult to spot in the moment, especially when the caller sounds legitimate and already knows some of your personal details.

In this month's newsletter, we look at how these scams work, what warning signs to look out for, and most importantly, how to protect yourself.



What is a bank impersonation scam?

A bank impersonation scam is where a fraudster contacts you pretending to be from your bank, building society, or even the police or a fraud investigation team. Their goal is to convince you that your money is at risk. They will often claim that:

- Your account has been hacked or accessed fraudulently
- Suspicious payments have been made from your account
- Someone is trying to steal your money right now
- Your account needs to be “secured” urgently

However believable the caller sounds, they are NOT from your bank, the police, or a fraud investigation team – they are part of a criminal gang trying to scam you. Their aim is to create panic and urgency, so you act quickly without thinking. You may be told to move your money into a “safe account”, but this is not safe – it belongs to criminals.

How the scam usually happens

These scams can start in several ways, including:

- A phone call claiming to be your bank’s fraud department
- A text message warning of suspicious activity
- An email asking you to “verify” your account
- A follow-up call after you receive one of these messages

Increasingly, scammers use “spoofed” phone numbers, so the call may appear to come from your bank’s genuine number, making it more convincing. The caller may sound professional and reassuring and may already know basic details about you, such as your name, address or bank. This information may come from data breaches or other sources. If you engage with them, they will use the conversation to build a story designed to make you feel anxious and act quickly.



Common phrases used by scammers

Fraudsters often use similar language patterns. You may hear things like:

- “We’ve detected unusual activity on your account”
- “Your money is at risk – we need to secure it immediately”
- “Do not hang up – this is urgent”
- “You must transfer your funds to a safe account”
- “We will stay on the line while you complete the transfer”

They may also claim that your cooperation is helping an investigation. A key tactic is keeping you on the phone so you do not have time to check independently.



What banks (and the police) will NEVER do

It is important to remember that genuine banks and building societies will NEVER:

- Ask you to move money to a “safe account”
- Ask for your full PIN or online banking password
- Ask you to withdraw cash and hand it over to a courier or “bank inspector”
- Pressure you to act immediately over the phone
- Ask you to keep the call secret

Importantly, the Police will also never:

- Contact you unexpectedly asking you to assist with an investigation in this way
- Ask you to withdraw cash or purchase items for an investigation
- Send a courier to collect money, bank cards, or valuables from your home

If you are ever asked to do any of these things, it is almost certainly a scam.

No genuine bank or police officer will ever ask you to move or hand over money in this way.

Why these scams are so effective

These scams work because they are designed to trigger strong emotional reactions:

- Fear – your money is at risk
- Urgency – you must act immediately
- Authority – the caller sounds official and knowledgeable
- Confusion – complex explanations make it hard to think clearly

Fraudsters are skilled at keeping people on the phone and preventing them from speaking to family or contacting their bank directly.



Staying safe with texts, emails and online forms

Scammers also use texts, emails and fake websites to trick people into sharing personal information. Never enter bank details, passwords, or personal information into links you receive unless you are certain they are genuine. If in doubt, go directly to the official website or use a trusted number.

Be cautious with online surveys too, as some are used to gather personal details that can later be used for scams.

How to protect yourself



There are simple steps you can take to stay safe:

1. Stop and think

'Take 5' - Pause before responding to any unexpected call or message about your money. If in any doubt, speak to a friend or family member first.

2. Never act under pressure

A genuine organisation will never rush you.

3. Hang up

If in doubt, end the call. This will not offend a genuine bank.

4. Call your bank directly

Use the number on your bank card or statement or dial 159.

5. Talk to someone you trust

Fraudsters often try to isolate people. A second opinion helps.

6. Remember

Your bank will not mind - They would rather you hang up and check than stay on the line with a scammer.



Protecting yourself from card fraud (cash machine skimming)

Skimming is a type of card fraud where criminals secretly capture the information stored on your bank card. It most commonly happens at cash machines or fuel pumps, where a small device is attached to the card reader.

Criminals may also use a hidden camera or fake keypad to capture your PIN. Once both are stolen, the information can be used to clone your card or make unauthorised withdrawals. Skimming devices are designed to be discreet but look out for anything loose or unusual on the machine. Always cover your PIN and use cash machines inside bank branches where possible. Checking your bank statements regularly can also help you spot suspicious activity early.

What to do if you think you've been targeted

If you think you may have been contacted by a scammer:

- Contact your bank immediately using their official number or 159
- Report it to [Report Fraud](#)
- Do not feel embarrassed – these criminals are highly skilled

Being targeted is not your fault.


Final thoughts

Bank impersonation scams are becoming more sophisticated, but the warning signs remain consistent: urgency, secrecy, and requests to move money.

Your bank will never ask you to move your money to protect it. The police will never ask you to transfer or hand over money as part of an investigation.

Pause, check and verify before taking action.

If you are affected by the content of this bulletin, you can talk to us. Our Scams Awareness and Aftercare Team can offer free support, advice and guidance. Contact our team today on:

 01625 612958 (OPTION 5)

 scams@ageukcheshire.org.uk

