



How to protect yourself from fraud

Fraud is everywhere, we are all at risk of losing our money every day.

Criminals are constantly finding new ways to trick you out of losing your money. They need you to fall for their tactics for their financial gain. We wouldn't give the keys of our home to just anyone so we should never do the same with our personal and financial information.

Read Brian's story:

Brian received a text that he thought was from AIB asking if he made a transaction to an online retailer for £499. The text also advised that if this message wasn't meant for him to contact the number provided. Brian had not made a transaction, so he rang the number in the text. He was told that it was a fraud message and was asked for his log in details and codes from his card reader to cancel the transaction.

Without Brian knowing it, the text was a scam and he had called a fraudster who now had all his details and took £9950 from Brian's account.

How do you protect yourself from fraud?

Do not trust any out-of-the-blue messages, calls or emails. Take a moment and ask yourself, could this be fraud? It only takes a split second to be caught off guard and one mistake can have serious financial consequences.

Fraudsters are using genuine bank, utility and phone company names to make the scam look legitimate. The most common way they do this is by sending you a text message containing a link or a phone number to call. These messages ask you to act urgently to secure your account, pay a fee, or stop fraud. Often these messages are followed up by a phone call. They may even use technology to mimic a genuine phone number.

Take a moment and ask yourself if this could be fraud. Don't click on a link and provide personal and financial information. Contact the sender through a trusted platform to check if the request is genuine. If you receive a phone call, hang up and call them back on a number from their genuine website.

We use one-time passcodes, card readers and face biometrics to protect your account. AIB will only ever text you to verify transaction by pressing 1 to confirm, or 9 if you don't recognise it.

We will never call or email and ask you to give us codes or take a selfie. We will never include a link. We will never send an employee, courier or taxi to your home to collect your cards.

For more information on common frauds and how to protect yourself, visit our security centre aibni.co.uk/security-centre.

Be Fraud Aware

We want to help you understand more about how to protect yourself and your bank account from fraud.

Fraudulent texts:

Criminals can make fake text messages look like they come from us. They can even insert these fake messages into genuine text conversations we are having with you.

One way of spotting a scam is that our web address will have .co.uk at the end. If it has any other ending like .com, it is definitely a scam.

Be careful and never click a link in a text message - even if it appears to be part of a conversation with us. We don't put links into our text messages.

Fraudulent phone calls:

Criminals can call you pretending to be us. They can even mimic our phone number. But remember:

We will never text you a One Time Passcode to cancel a transaction.

We will never ask you to get a code from your Card Reader to cancel a transaction.

We will never ask you not to log back into your account.

You should not share a One Time Passcode code or Card Reader code with anyone if you get an unexpected call or text message, whoever they say they are, **even if they say they are from our fraud team.**

We will never call you to ask for a code we have sent to you, or to ask why you didn't complete the process in the text message.

These codes are the way to make money leave your account. Never share them with anyone including bank staff

Remember: AIB staff including those working in our Fraud teams will **NEVER** ask you for security information, or for you to transfer money out of your account in any of our email, phone or text communications.

If you do receive an email, text or a phone call that claims to be from AIB and asks you for personal information or to take urgent action, **please do not respond, do not follow the instructions and report it via the form at** aibni.co.uk/security-centre/contact-us/fraud-form or call 028 9034 6034

(8.30am to 5pm Monday to Friday, including bank holidays). We may record your call and there may be a charge from your service provider to call us.

If you notice anything suspicious on your bank account or you believe you have been a victim of fraud, contact us 24/7 on Freephone number 0800 0391 140.

For more security advice and pointers on how to protect yourself from Fraud, do refer to the Government 'scamwiseni' and 'TakeFive' initiatives, and to the list of AIB contact telephone numbers on our secure website www.aibni.co.uk.



The AIB logo and AIB (NI) are trade marks used under licence by AIB Group (UK) p.l.c. incorporated in Northern Ireland. Registered Office 92 Ann Street, Belfast BT1 3HH. Registered Number NI018800. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.