



28th March 2025

Reported cases of phone call fraud up almost 80% in 2025

- AIB urges people to be fraud aware as fraud instances continue to increase.
- Fraudsters make every effort to steal your money – don't let it happen.
- Case study – phone call to AIB saved one customer from losing €40,000 to fraudsters

AIB is urging our customers to remain vigilant against the threats of financial loss associated with phone call fraud. In January and February 2025 we have seen a sharp increase in reports of phone call or vishing fraud, with overall vishing increasing by 79% compared to the same two months last year. These fraud attempts are targeting both personal and business customers.

Fraudsters are using phone calls more often to target unsuspecting customers. These calls claim to represent reputable companies and financial institutions.

Common tricks used on these calls include:

- offering a refund
- claiming to stop a payment that is fraudulent
- or even advising they are going to fix an issue with your broadband.

Fraudsters often ask you to download software to your device or to visit a 'secure' website. By following the caller's instructions, you are allowing them to take control of your device and by providing codes are allowing them to access your accounts and take money from you.

Businesses need to be aware of the threats associated with phone call fraud and ensure all staff who manage their accounts are aware of the risks of giving away information or downloading software. One of our business customers, who wishes to remain anonymous, was recently a victim of vishing fraud and has shared their story to alert other customers of these scams.

One customer's story

On the 17th February, the customer's business received a call to its landline. The caller who introduced himself as Gavin from AIB's fraud team, told the customer that there were two payments due to leave their account. To make the story seem legitimate, Gavin provided amounts and reference numbers for these payments. When our customer told him she had not made these payments, 'Gavin' advised her with a sense of urgency that he would be able to get them cancelled but would need to take our customer to a secure webchat facility. He advised them that this was for their security and swift action was required.

Our customer was told to open the browser on her PC and type in a web address. In the moment and out of panic that fraud was occurring on her account, our customer followed Gavin's instructions and visited a fake AIB website. What she didn't realise was that this site contained software that allowed

'Gavin' to access her PC. Unknowingly our customer also provided security codes to the caller which allowed a payment of €41,000 to be made.

Gavin then called AIB's Customer Engagement Centre posing as our customer requesting the payment be processed without delay. The AIB staff member immediately knew something was wrong, ended the call and contacted our genuine customer.

While this was a good outcome for our customer, this is not always the case. Customers need to be aware of the following to safeguard both their personal and financial information:

- End any unexpected calls. Contact the company on a known and trusted contact number to verify the legitimacy of the call.
- Never visit websites or download software to your device on the back of an unexpected call.
- Never provide login information, one-time passcodes generated by text message or codes from your Digipass or card reader device. These codes allow access to your account and allow money to be moved from it.
- Never move funds to a 'safe' account if requested to do so.
- Call the 24/7 AIB fraud helpline if you think you have been scammed.

Tips to protect your money and avoid being scammed

AIB's Head of Financial Crime, Mary McHale said "Fraudsters will use any means to steal your money. They will pose as legitimate companies or bank staff to trick you into downloading software and providing personal and financial information. They may even mimic a company's genuine phone number. We urge people not to let their guard down and remain vigilant. Take a moment and ask yourself, could this be a scam? End the call immediately and verify its legitimacy on a known and trusted phone number.

Where customers have been scammed, we will deal sympathetically with them on a case-by-case basis. At AIB, we have a strong record in protecting our customers from fraud and we are continuously investing to enhance our fraud monitoring systems in response to new and existing fraud trends, and to educate our customers via online messaging, emails, and targeted social media alerts. Our fraud helpline is open 24/7, seven days a week to support our customers when they need us. We also work closely with industry stakeholders including telecommunications companies, the Banking and Payments Federation of Ireland (BPF), and the Gardaí to detect and report fraud trends, as it's only by communicating and coordinating across the whole of society that together we can be effective in combating these criminals."

For more information on the latest frauds and scams visit the security centre on the AIB website or call our 24/7 seven days a week fraud support line on 1800 24 22 27.



Pictured: Head of Financial Crime Mary McHale. Credit: Shane O'Neill, Coalesce

Media queries: paddy.x.mcdonnell@aib.ie 087 7390743