27th June 2025

Phone fraud or vishing activity up by almost 300% as top five frauds revealed – AIB Fraud Trend

- Vishing activity up 297% (based on the value of payments reported as fraudulent)
- Losses associated with customers compromising their log-in details is up 67% (among frauds which are not smishing or vishing ones)
- Wait a sec-double check. Tips on how to ensure you don't fall foul of top five frauds this summer

AIB's latest Fraud Trend report reveals a surge in vishing activity for January to May. Between January and May 2025 we have seen a sharp increase in reports of phone call or vishing fraud, including text message fraud, with attempted and successful fraudulent activity up 297% compared to the same period last year (based on the value of payments reported as fraudulent).

AIB's data also shows a 6% increase in customers falling victim to smishing/vishing scams – typically phone calls that often follow after a customer responds to a fraudulent text message – based on the requirement to have new login details issued. Meanwhile losses associated with customers compromising their login details is up 67% (among frauds which are not smishing or vishing ones).

Top Five Frauds

AIB is outlining the five most common scams fraudsters are carrying out to fool people into handing over access to their money from April to June 2025, as well as how to protect yourself and your money from them. Customers who fall victim to text message fraud and safe account scams often receive vishing calls as part of the scam.

1. Text Message Fraud

Text message fraud, also known as SMS phishing or smishing, continues to be a major threat and the crime that's most commonly perpetrated by fraudsters. Scammers send convincing messages that appear to be from reputable sources, such as banks, delivery companies or Government agencies, tricking recipients into providing personal information or clicking on malicious links. Our advice is to never click a link in an unexpected text message or call the number provided. If in doubt contact the sender on a known and trusted number to verify its legitimacy. You should never provide log in details, security details such as one time passcodes, card reader codes or selfies.

2. Safe Account Scams

Safe account scams involve fraudsters posing as bank officials who call and inform victims that their accounts have been compromised. They then persuade victims to transfer their funds to a 'safe' account for protection, which is often their own account, and often in other financial institutions. The funds can then be moved onto a mule account. These safe accounts are, in fact, controlled by the scammers, resulting in the victims losing all transferred funds. We will never call you and ask you

to move your money to a new account for safe keeping. If you receive a call like this, hang up immediately.

3. Investment Scams

Investment scams have surged in 2025, with perpetrators offering lucrative returns on fake investment opportunities. These scams often target individuals seeking to grow their savings quickly, using convincing pitches and professional-looking websites. Victims invest substantial amounts of money, only to realise later that the promised returns are non-existent and their funds have been stolen. Always ask yourself, is this too good to be true?

4. Holiday Scams

As we come into peak travel season, we have also seen a rise in holiday scams. Scammers create fake travel websites and offers, luring victims with attractive deals on flights and accommodation. Once payments are made, victims discover that their bookings are fraudulent and their dream holidays are ruined. These scams not only cause financial loss but also lead to immense disappointment and frustration. Always book your holidays through reputable providers, research accommodation to ensure it actually exists and don't part with your money unless you are fully satisfied. These scams aren't just advertising foreign holidays, but Irish ones too.

5. Purchase Scams

Shopping online can be convenient, but it also comes with several risks. One of the main concerns is the possibility of encountering fraudulent websites or sellers who may take your money without delivering the promised goods. Additionally, there's the risk of your personal and financial information being stolen through phishing scams or insecure websites, leading to identity theft and financial loss. Another threat is the potential for receiving counterfeit or substandard products, which can be disappointing and harmful. To mitigate these risks, it's essential to shop from reputable websites, use secure payment methods, and stay vigilant for any signs of suspicious activity. Always ask yourself, is this price too good to be true?

Mary McHale, Head of Financial Crime said "AIB is today outlining the five most common ways criminals are targeting you to steal your money. We want customers to be alert, check the advice on our AIB security centre, and to take a moment to ask yourself, could this be a scam? That's why you should wait a sec and double check.

Where customers are scammed AIB deals sympathetically with them on a case-by-case basis. We are continuously investing to enhance our fraud monitoring systems in response to new and existing fraud trends. 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 (BPFI), 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."

Top Tips to keep your personal and financial information safe and secure:

1. **Stay Informed**: Keep up with the latest scams and how they work. Knowledge is your first line of defence.
2. **Verify Sources**: Always double-check the legitimacy of any unsolicited messages, calls, or emails. If something seems off, it probably is.
3. **Protect Personal Information**: Never share your personal or financial information unless you are sure of the recipient's identity and legitimacy.
4. **Use Strong Passwords**: Create strong, unique passwords for your online accounts and change them regularly.
5. **Be Sceptical of Unusual Requests**: If someone asks you to move money to a safe account, end the call and don't act on their request

For more information on how to protect yourself from fraud, visit our security centre on aib.ie. Here you will also find our contact information including our 24/7 fraud support line on 1800 24 22 27.

Media enquiries: paddy.x.mcdonnell@aib.ie 087 739 0743