27th September 2024

AIB urges people to be vigilant as instances of text message fraud increase

Multiple 'money mule accounts' being added as payees to customers' accounts by criminals purporting to work for bank fraud teams

AIB is advising customers that it will never contact them by text message or phone call requesting their banking login details, passcodes or PINs. In recent weeks scammers are using sophisticated technology to insert fraudulent text messages into legitimate message threads. This text will contain a link to a fake website or a phone number which links to a fraudulent call centre.

Other genuine financial institutions, courier services, Government agencies and utility companies are also being targeted in this scam which follows a similar pattern to our customer Sarah's story:

Sarah was at home after work when she received a fraudulent text message which was inserted by criminals in a thread of otherwise genuine messages from AIB advising her that a direct debit had been set up and would leave her account. This message was unexpected and included a phone number for her to call. As Sarah had not requested a direct debit to be set up on her account she was extremely concerned and called the phone number without delay.*

Someone purporting to be named Mark answered the call and claimed he worked in the AIB fraud team. He assured her that he would assist in cancelling these fraudulent transactions. Thankful for the assistance, Sarah did not suspect that this was a bogus AIB staff member and provided all her login and personal information to Mark. On the call Mark advised Sarah not to log into mobile or online banking as this could prevent the fraud from being stopped. Sarah did not realise that Mark was in fact a fraudster who was adding numerous money mule accounts as payees to her account, using the security codes she provided. Mark who had all Sarah's login details was logged into online banking and was in the process of emptying her account.

Sarah is just one example of how fraudsters are targeting people by instilling a sense of fear and panic with the tone of these messages.

AIB's Head of Financial Crime, Mary McHale said "fraudsters are becoming more and more sophisticated, and we have seen an increase in the number of cases of this kind of scam in recent weeks. AIB will never ask customers to log into a website or phone a number contained in a text message. We urge customers to end any conversation where someone is purporting to be from their bank and is requesting security details including security codes, one time pass codes, or even to supply images of their face.

Fraud can be very distressing for customers as it often involves significant amounts of money. These scams can be very sophisticated, and criminals go to great lengths to defraud by spending hours on phone calls and even calling victims back over a number of days.

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. 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 we will together be effective."

We're all aware of frauds and scams, having received fraud prevention messages and warnings from our bank, on social media, in newspapers, on TV and on radio. However, it only takes a moment to get caught off guard and if we make a mistake, it can have serious financial consequences.

Top tips to be fraud aware:

- Everyone should keep the phrase 'don't click on the link' in their minds.
- Take a moment to ask yourself 'is this legitimate?', before reacting to a call or message and if in doubt, err on the side of caution and do not respond.
- Make yourself aware of current fraud threats by regularly checking your bank's security centre on their website.
- Do not call any number provided in a text or email message. Search and confirm the phone number using the bank's website.
- You can also ensure any website you use is secure and genuine by checking for the padlock symbol to the left of the web address. If it's not there, beware.
- If you think you have been a victim of fraud, contact your bank immediately and report it to the Gardai.

ENDS

Contact louise.y.kelly@aib.ie, 00353 87 2161545