04 December 2024

Text message and phone call fraud most common scams of 2024, AIB reveals

‘Smishing’ accounts for 94% of all fraud cases from January to October this year

- **AIB urges people to be fraud aware this Christmas**
- **Fraudsters won’t take time off - so don’t let your guard down this festive season**

As we head into the festive season and 2024 draws to a close, AIB is urging customers to remain vigilant against fraud as it can affect anyone at any time, particularly as people take time off to relax over Christmas.

Criminal activity continues even during the festive season and AIB has compiled a Christmas countdown of the top five most common fraud methods we’ve seen in 2024.

1. **Text message fraud**

Fraudulent text messages claiming to be from reputable banks, delivery or utility companies are by far the most common type of fraud, with 94% of all cases between January and October 2024 ‘smishing’ related. Take a moment and ask yourself does this seem legitimate? Don’t click the link in the text message or share your personal or financial information.

Often these messages are followed by a phone call claiming to be AIB, sometimes even using our actual phone number. End the call immediately. We will never call you and request security codes sent by text message, push message or from your card reader. We will never send a taxi or courier to collect your physical card, PIN or any security details. We will never ask you to provide a selfie through our mobile app after receiving a call or text message.

2. **Phone call fraud**

Fraudsters often use phone calls to get your personal and financial information for their own financial gain. They may pretend to be from a legitimate company and may even display a genuine phone number. Common tricks used on these calls include offering to fix an issue with your broadband or offering a refund. They may try to take control of your device. Never download software or apps that they suggest onto your computer or mobile phone as this will allow fraudsters access to your information.

End any unexpected calls. Call the genuine company back on a known and trusted number to verify the call.

3. **Investment fraud**

Investment frauds and scams are on the rise, with criminals using social media to advertise highly profitable investments. These ads often use advanced technology to appear legitimate.

Always ask yourself, is this too good to be true? Such high return investments are usually not genuine. Before investing your money take some time to research the provider, verify their existence, and that they are regulated and always seek independent financial advice.

4. **Purchase scams**

Online shopping is convenient and popular, especially at Christmas time, but criminals can clone genuine websites to offer fake discounts to target unsuspecting customers. This can happen with any site, including clothing, homewares, or heavy goods vehicles such as diggers, campervans and boats. These cloned sites often look and feel genuine.

When shopping online, particularly at busy times like Christmas and the New Year sales, check for a padlock symbol in the address bar, research the site for negative reviews, and verify contact details. Avoid direct bank transfers. Ask yourself, is this price too good to be true?

5. **Money mules**

Being a money mule is a criminal offence.

Criminals use other people's accounts to transfer stolen money to conceal their crime. They can trick anyone into using their accounts. Without access to your account, criminals will not be successful.

They may approach you online, in person, on social media or through fake job adverts asking to move money through your accounts or to open a bank account in your name for them. They may even offer you some money as payment. This use of your account, even if you don't know where the money has come from or is going to, means you are becoming a money mule. This may result in your bank account being closed or a criminal conviction for money laundering.

Parents should also be aware that teenagers and young adults are often targeted by criminals, with the promise of quick cash so sharing this information with family members can also be helpful.

AIB is also urging **businesses** to exercise caution as a number of scams are in circulation. Fraudsters are currently targeting businesses using impersonation tactics and can claim to be your customer or supplier. You may receive an unexpected credit into your account, which will be followed up by a phone call or email. The caller or sender of the email will claim to be your customer and advise the payment you have received, was made in error. They will request that you transfer the funds back to them but will provide a different IBAN number.

Don't act on these payment requests as your customer may also be a victim of fraud. Verify all payment requests on a known and trusted contact number. Do not use the contact details contained in an email or email attachment.

AIB's Head of Financial Crime, Mary McHale said "as the festive season gets well underway, we know fraudsters will be hoping to take advantage of people as they relax and take some time off with friends and family. We are urging people not to let their guard down and to remain vigilant, especially over Christmas and the New Year when many of us will be shopping online.

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.

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 together we can be effective in combating these criminals."

For more information on the latest frauds and scams visit the security centre on our website.

ENDS

Contact louise.y.kelly@aib.ie. 087 2161545