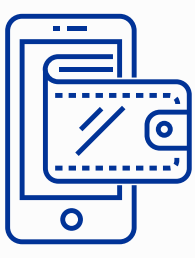
PermataBank

Scams Using Virtual Accounts

In addition to the fraudulent mode that uses a bank account, there are also fraudsters who request people to send the money through a virtual account. Before discussing further, you need to know the meaning of the term virtual account. Virtual account is a cash management service that consists of 16 unique and specific numbers to assist companies that are PermataBank customers to identify fund receipts with a fast and accurate reconciliation process. The issuance virtual account number is carried out by the company to be given to its customers (individuals or non-individuals) as the account number for the recipient's destination with the naming according to the customer's name. The company can also cooperate with its customers without the involvement of the Bank.

Furthermore, virtual account can be used by company customers (financial providers) as a medium for receiving funds from a particular transaction. There are 2 types of virtual accounts:



Static Virtual Account

Virtual account numbers that can be used repeatedly, for example virtual account numbers for DANA, ShopeePay, GoPay, OVO, etc.

Dynamic Virtual Account

A virtual account number that can only be used for one transaction, for example when making payments through a virtual account on an online/e-commerce website, for example through a Facebook merchant.

Because virtual accounts can be used as a medium for receiving funds, many fraud modes occur using virtual accounts. The scheme being used are also varied, as conveyed in previous educational materials, fraudsters can use modes such as:

1

Claiming to be a relative or friend

Tips: Get to know your speaking style/language. Usually, fraudsters pretending to be somebody close to you, and they are currently in a disaster or a state of urgency so they need funds quickly.

2

Invest through social media (WhatsApp, Telegram, etc.)

Tips: Check investment offers legally and logically. Usually, investment offers promise fantastic profits and invite participants to send some funds through a virtual account. The investments offered are unlicensed and the promised investment returns are far from expectations or even non-existent. There is also a scam scheme under the guise of investment, the most popular and simple is the Ponzi scheme. A promoter or online platform that lures potential investors with a very high rate of return.

3

Fake lucky draw

Tip: Be alert and think logically. If you have never participated in a certain reward program, it is better if there was a caller or chat who will give you a gift because in the end fraudsters will ask for your banking data and ask for the number of funds to withdraw the prize.

4

Online shopping or fake online shop

Tips: do a crosscheck in the comments section and avoid paying outside the official payment method from the online store. Usually, fake online stores disabling comment section and display fake testimonials in the form of screenshots of WhatsApp chat, or even no testimonials at all.

The smart way to avoid the above fraud mode is:

1. In the e-wallet application (which uses a virtual account) there is a feature to be able to change the name of the e-wallet account owner, this is then often used by fraudsters to do social engineering (fraud). Before transferring funds, it is better to first contact the owner of the e-wallet account to minimize fraudulent actions.
2. If there is a message that says you won the lottery program, make sure to call the bank/company call center. Check whether there is a lottery program or not.
3. Ask financial and investment experts/experts or check financial products with the Financial Services Authority (OJK) customer service before deciding to participate in investment offers.
4. Pay attention to the name of the contact and the conversational style of the message sender. When in doubt, you should just block the contact.
5. Be careful with profile pictures, for fear of fraudsters using the photo on other social media accounts for criminal purposes.
6. If it was indicated that you are experiencing fraud, immediately contact the call center of the bank/virtual account owner company for further checking and include evidence of reporting in the form of a report letter from the police, proof of transaction, and statement letter.
7. If the virtual account was considered a fraudulent account, immediately report it through CekRekening.id, owned by the Ministry of Communication and Information of the Republic of Indonesia.

For more information, please contact:

care@permatabank.co.id | PermataTel 1500-111 | 021 - 29850611

@PermataCare | @permatabank | PermataBank