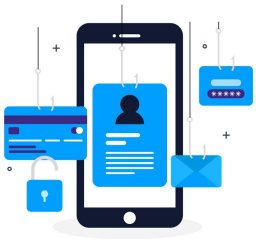

Stay tuned! Fraudulent SMS

A new fraudulent scheme has been detected that aims to extort data from users of digital channels

A new fraudulent scheme has been detected, which aims to extort data from users of digital channels, which are personal and non-transferable.

WHAT SHOULD I DO:

- Do not open the link
- Do not provide any data
- Immediately delete the message.

Remember that ICD Bank:

- **It does NOT** require software installation or update
- **DOES NOT** send SMS with links
- **DOES NOT** send Email with links
- **DOES NOT** request the full Multichannel Code (the 7 digits)
- **DOES NOT** ask for mobile number
- **DO NOT** request, by phone or other means, the Authorization Code sent by SMS
- **DOES NOT** simulate transactions with Customers

The only information we request when you access ICD Bank is:

- User Code
- 5 random digits of the Access Code

Some operations, via the Site, may request an Authorization Code. This code is exclusive and only valid for the operation you are requesting. The Code is sent by SMS to your mobile phone.
The Access Codes to ICD Bank are personal and non-transferable, memorize them and do not register them in unsafe places.
For security reasons, the Site and App include session timeouts and automatically cease if they are inactive after a period of time.
Whenever you detect any situation that seems suspicious or needs clarification, contact us through the Customer Support Line*