Social Engineering

HOW TO PROTECT YOURSELF FROM FRAUD AND FINANCIAL SCAMS

In compliance with SARB Regulation 027/2023) and ensuring transparency in our relationship with our clients, the Bank of China Brazil Conglomerate emphasizes the pillars of its relationship with elderly customers.

WHAT IS SOCIAL ENGINEERING?

A large proportion of scams are linked to social engineering, which occurs when customers are tricked into giving their codes and passwords to criminals. Using persuasion techniques, the scammers obtain information that can be used for unauthorized access to computers or banking information. These situations are even more frequent among the elderly.

LEARN ABOUT THE MAIN APPROACHES OF THE SOCIAL ENGINEER:

Fake Websites: 1. Imitation of the websites of major institutions, aimed at misleading the victim into believing that they are reliable and legitimate**. 2.** Websites with attractive content so that the victim is persuaded to provide personal data for registration purposes or by offering discounts and coupons.

Emails: sending emails that appear to come from reliable sources in order to obtain personal data or sensitive information.

Social networks: publications that have no control over their display to third parties are available for viewing by any user and can be a very useful tool for applying scams, as the social engineer will already know a little about you.

Instant messaging applications: dissemination of links and malicious files via instant messaging applications. Make sure that the content and links you receive are from known and trusted contacts.

Telephone and SMS: the scammer identifies themselves as a representative of a fake call center for telephone companies or well-known institutions such as banks, credit card companies or government authorities. During telephone contact, for example, they use persuasion and convincing techniques to induce the victim to confirm personal details, passwords, tokens, card numbers or sensitive corporate information. Another technique used is to send text messages via instant messaging applications or SMS, inducing the victim to access a link.

In person: the fraudster contacts the victim posing as a fake employee of the Financial Institution or company with which the Client has a relationship. The scammer informs them that there are irregularities in the account or that the data entered is incorrect. They then ask for the victim's personal and financial details. With the data in hand, the scammer carries out fraudulent transactions on behalf of the client.

HOW TO PROTECT YOURSELF FROM SOCIAL ENGINEERING?

• Do not provide personal data, passwords or sensitive information by telephone, e-mail, social networks or instant messaging applications.

• Be aware: Bank of China Brasil does not request confirmation of personal data relating to bank accounts, passwords and cards by telephone, SMS, e-mail or other means. Never provide data to someone who identifies themselves as a call center operator.

• Do not reply to messages from unknown companies or institutions by any means.

• Avoid opening emails, instant messaging applications or SMS, and clicking on attachments or links sent by strangers.

• Always activate the “two-factor authentication” security function on your internet accounts that offer this option: email, social networks, applications, operating systems, etc.

• Be wary of very generous promotions or promises of easy money on the internet.

• When creating a profile on social networks, define your preference for privacy settings for your posts, prioritizing them whenever possible for only friends or certain groups and be wary of excessive virtual exposure, as the information available can attract criminals and put you and your family's safety at risk.

• If you receive a suspicious call, don't pass on any of your details. End the call, wait 5 minutes and contact your bank's call center through the official channels - the ones you can find on the institution's website. The waiting time is important so that your call is not intercepted by fraudsters.

CUSTOMER SERVICE CHANNELS:

• **Hearing or Speech Impaired:** 0800 940 0649

• **Call Center:** For queries and information.
Telephone: 0300 010 0242
E-mail: central@bocfinanceira.com.br (for services relating to vehicles or INSS Payroll Loans) central@bocbanco.com.br (for other Payroll Loan and Credit Card contracts)

• **Collection:** For payment of overdue slips, overdue contracts or any other problem relating to collection.
Telephone: 0300 010 0242
E-mail: cobranca@bocfinanceira.com.br

• **Customer Service:** For complaints, information and cancellations.
Telephone: 0800 725 0048
E-mail: sac@bocbrasil.com.br: for contracts relating to vehicles or INSS Payroll Credit. sac.cdc@bocbrasil.com.br: for other Payroll Credit contracts, Credit Cards and Individual and Corporate clients.

• **Ombudsman's Office:** If you have already contacted SAC but would like to have your service reassessed.
Telephone: 0800 725 2242
E-mail: ouvidoria@bocfinanceira.com.br

• **In-Person Service**
Entrance on Avenida Paulista, 901
Monday to Friday, from 10 a.m. to 4 p.m., except national holidays.

• **Correspondence:**
Alameda Santos, 960, 13th, 14th, 15th and 16th floors, Cerqueira César - CEP: 01418-002.

You can always count on BOC Brasil!

中國銀行 (巴西)
BANK OF CHINA (BRASIL) BANCO MÚLTIPLO S/A
www.bocbrasil.com .br

BANK OF CHINA BRASIL FINANCEIRA
www.bocfinanceira.com.br