#EstejaAtentoNãoSeja**Vítima**

ESTEJA ATENTO A **MENSAGENS FRAUDULENTAS**

Estimado(a) Cliente,

O *phishing* é um tipo de acção fraudulenta que recorre ao uso de mensagens de *SMS* ou de *e-mail* que apresentam ter origem no BAI, mas que efectivamente provêm de impostores.

Conheça aqui as várias tentativas de fraude, siga as boas práticas que recomendamos e mantenha-se sempre informado sobre os nossos conselhos de segurança. Desconfie permanentemente de mensagens com o seguinte teor:

- Pedido de informações pessoais;
- Pedido de informações bancárias;
- Recomendação de acções urgentes porque as suas credenciais de acesso poderão ser bloqueadas.

PRESTE ATENÇÃO AOS FORMATOS DE E-MAIL, ELES TÊM O SEGUINTE FORMATO:

Primeiro e o último nome@nome da empresa.com /.co.ao/.org e mais.

Por exemplo: **marisa.tavares@bancobai.ao**

QUAIS SÃO AS CONSEQUÊNCIAS CASO SEJA VÍTIMA DE UMA FRAUDE?

- Acesso indesejado à sua conta;
- Informações sobre os seus cartões, que podem ser usadas para compras e outros fins.

DESCONFIE SEMPRE DE MENSAGENS EM QUE LHE PEÇAM:

- Para validar dados de autenticação;
- Para validar dados de operações de pagamentos;
- Para instalar um aplicativo no seu telefone ou PC.

COMO PODE MANTER-SE SEGURO

- Reporte todas as tentativas de fraude por SMS, chamada telefónica, e-mail ou por outra forma que lhe pareça suspeita.
- Apague as mensagens suspeitas porque corre o risco de aceder um link por engano.

ESTEJA ATENTO AS SEGUINTES MENSAGENS SUSPEITAS:

DESCONFIE DOS LINKS ABAIXO:

http://baiangola.ao
http://bancobaieuropa.com
bancobai-support@trex
bai_support@onlin
bancobai-support@moneyi
http://bancobai.net

EM CASO DE NOTIFICAÇÃO DE MENSAGENS SUSPEITAS, POR FAVOR LIGUE PARA:

Linha de Atendimento das 7H00 às 23H00

923 169 390

Lembre-se que o BAI não solicita informações pessoais ou bancárias como: **nome**, **endereço**, **residência**, **código de acesso**, **número de cartão**, **por estas vias**.

25 anos 1996 - 2021

BAI
Confiança no Futuro