interweb

Gerado a 13/11/2026 18:08

BASE DE CONHECIMENTO · DOCUMENTO PÚBLICO

Golpes do código partilhado: proteger os seus clientes de quem lhes pede o código do SMS

Segurança

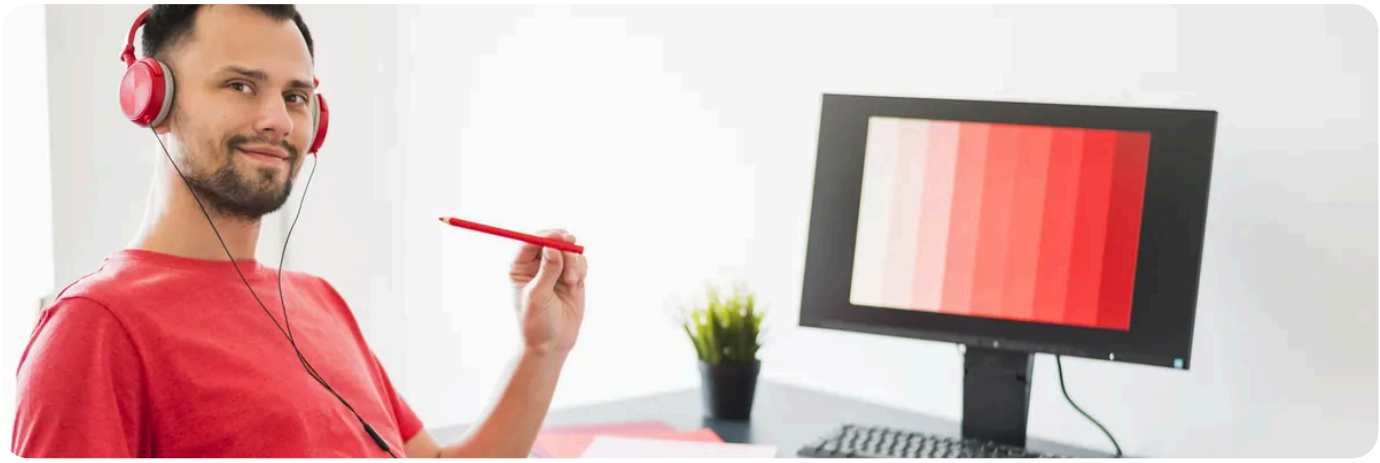
CÓDIGO	VERSÃO	PAÍS · IDIOMA
RLX-AO-KB-2650	v2026.11.13	Angola · Português

Interweb Angola
RLX Angola, Lda. · Grupo RLX Holdings
NIF 500 260 5724 · Matrícula 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/2650

Golpes do código partilhado: proteger os seus clientes de quem lhes pede o código do SMS

Segurança Criado em **13 de novembro de 2026** 3 min de leitura



A resposta curta: o código por SMS só protege enquanto ficar no telemóvel do cliente. O golpe mais comum não ataca a sua API, ataca a pessoa: alguém liga ou escreve, finge ser da sua empresa, do banco ou da operadora, e convence o cliente a ditar o código. Do seu lado, a defesa está no texto do SMS, na regra de que ninguém da sua equipa pede códigos e no que faz quando um cliente diz que caiu.

Como costuma acontecer

A história que contam	O que o código está, na verdade, a aprovar
«Enviámos-lhe um código por engano, pode ler-mo?»	A entrada na conta do cliente, ou a mudança do número
«Para cancelar esta compra, diga-me o código que recebeu»	A própria compra, ou uma transferência
«Ganhou um prémio; para o receber, confirme o código»	Um pagamento ou um novo beneficiário
«Sou da equipa técnica, preciso do código para resolver o problema»	O acesso à conta

O que o seu SMS deve dizer

1. **Para que serve o código.** «Código 739204 para confirmar o pagamento» é muito mais difícil de usar num golpe do que «O seu código é 739204».

2. **«Não o partilhe.»** Duas palavras que a página do SMS de Verificação recomenda em todos os códigos.

3. **«Ninguém da nossa equipa o vai pedir.»** Se couber, é a frase que desmonta a chamada falsa.

4. **Quem envia.** O nome da sua empresa no início do texto e, se possível, um **Sender ID**: o cliente habitua-se a ver os seus códigos sempre com o mesmo nome.

5. **Sem ligações.** Um SMS de código não precisa de endereço nenhum. Um código com ligação parece-se demasiado com as mensagens falsas.

Um exemplo que cabe num SMS: `[EMPRESA]: código {code} para confirmar o pagamento. Não o partilhe. Ninguém da nossa equipa o pede.`.

A regra da casa, e quando um cliente cai

Escreva-a e ensine-a a toda a equipa: **nunca se pede um código ao cliente**, nem por telefone, nem por mensagem, nem no balcão. O código é escrito pelo cliente no seu site ou aplicação, e só aí. Os remetentes com nome não recebem respostas, por isso também não faz sentido pedir ao cliente para «responder com o código».

1. **Cancele o que estiver pendente** com `POST /v1/sms/otp/{id}/cancel` e trave a operação no seu sistema, se ainda não foi executada.

2. **Feche as sessões abertas** da conta e peça ao cliente que mude a senha.

3. **Confirme os dados de recuperação**: se o golpe serviu para mudar o número ou o e-mail, reponha-os com verificação de identidade.

4. **Registe o caso**, com a hora do código (`created_at` e `verified_at`), para perceber o padrão e avisar outros clientes.

Não use o código como prova de identidade ao telefone.
Pedir ao cliente que leia um código «para confirmar que é ele» ensina-o exactamente o comportamento que os golpistas exploram.

Um aviso depois de cada operação sensível
ajuda o cliente a reagir a tempo: «Foi confirmado um pagamento na sua conta. Se não foi você, ligue [TELEFONE].» Envia-se como SMS normal; ideias em **SMS transaccional**.

RECOMENDADO

Quer que os seus códigos digam claramente para que servem e quem os envia? Veja o SMS de Verificação.

Ver o SMS de Verificação →

VEJA TAMBÉM

- Escrever o SMS de verificação: o lugar do código, o seu Sender ID e caber numa só parte
- Confirmar pagamentos, levantamentos e transferências com um código por SMS: um código por operação
- Mudar o número de telemóvel de um cliente com segurança: confirmar o número novo antes de o gravar
- Entrada em dois passos com um código por SMS no seu site ou aplicação
- O que é o Sender ID: SMS que chegam com o nome da sua empresa em vez de um número
- Enviar códigos de uso único (OTP) por SMS com segurança: validade, tentativas e registos

interweb

Interweb Angola

RLX Angola, Lda. · Grupo RLX Holdings

NIF	500 260 5724
MATRÍCULA	26464-25/250724
SEDE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACTOS	info@interweb.ao · +244 942 011 191 · www.interweb.ao
HORÁRIO	2ª. à 6ª. Feira - 08 à 16 Horas Sábado & Domingo - Fechado

Versão online deste documento

RLX-AO-KB-2650 · v2026.11.13 · Gerado a 13/11/2026 18:08