

# Recebi uma mensagem suspeita. E agora?

E-mail, SMS, WhatsApp ou ligação pedindo dinheiro, senha, código ou clique. Antes de qualquer coisa, siga estes três passos.

## 1. Pare

Não clique, não responda, não pague, não instale nada. Nenhuma situação real precisa ser resolvida em cinco minutos por mensagem.

## 2. Pense

Eu esperava essa mensagem? Esse pedido faz sentido? Alguém está me apressando ou me ameaçando?

## 3. Confirme

Fale com a pessoa ou a empresa por um canal que **você** já conhece: telefone oficial, aplicativo do banco, ou a coordenação, pessoalmente.

## Sinais de que é golpe

### Pressa ou ameaça

Prazo curto, conta bloqueada, multa, processo, "só hoje".

### Pedido de senha, código ou dados bancários

Nenhum banco, órgão público ou empresa pede isso por mensagem.

### Remetente parecido, mas diferente

Endereço com letra trocada, domínio estranho, número desconhecido.

### Link ou anexo inesperado

Link encurtado, ou arquivo .zip, .exe e .html que você não pediu.

### Pedido de segredo

"Não comenta com ninguém", "resolve só você".

### Bom demais

Prêmio, reembolso, doação grande com uma pequena taxa antes.

## Nunca, em nenhuma hipótese

- Passar o código de 6 dígitos que chegou por SMS. É assim que clonam o WhatsApp.
- Informar senha, token ou dados do cartão por mensagem ou telefone.
- Pagar boleto sem conferir o beneficiário e o CNPJ na tela do banco.
- Instalar programa de acesso remoto a pedido de quem ligou.
- Enviar dados ou fotos das acolhidas por canal pessoal.

## Se você já clicou ou já pagou

- 1 Avise a coordenação agora. Ninguém leva bronca por avisar.
- 2 Guarde prints e não apague nada: são provas.
- 3 Troque a senha por outro aparelho e ative a verificação em duas etapas.
- 4 Se fez Pix, ligue ao banco e peça o MED (Mecanismo Especial de Devolução).
- 5 Registre boletim de ocorrência na Delegacia Virtual.

## Anote aqui, antes de precisar

Coordenação:

Gerente do banco:

Suporte técnico:

Polícia Militar: 190