

10 Dias Contra os Golpes



O guia simples para proteger
seu dinheiro, celular e dados.



Pare. Desconfie. Confira.
Só depois decida.



Proteja
seu dinheiro



Cuide dos
seus dados



Evite golpes
todos os dias



@edinaldodos90

Antes de começar



Golpistas não precisam necessariamente hackear uma pessoa. Muitas vezes, tentam convencê-la a entregar voluntariamente uma senha, código, informação ou dinheiro.



EM 10 DIAS, VOCÊ VAI:



Em 10 dias, você vai aprender a reconhecer sinais de golpe, verificar mensagens, links, pagamentos e contatos, proteger celular, WhatsApp e contas bancárias, evitar decisões tomadas por pressão, agir rapidamente depois de um golpe e criar uma rotina simples de segurança financeira.



A REGRA DE OURO:

Pare. Desconfie. Confira. Só depois decida.



O MÉTODO:

1



1. Entenda o golpe

2



2. Reconheça os sinais

3



3. Saiba o que fazer

4



4. Faça o exercício do dia.



Golpe pode acontecer com qualquer pessoa. Informação é a sua melhor proteção.





Dias 1 a 3: pare antes de comprar, transferir ou obedecer

DIA 1



Falsa venda



- preço muito abaixo do mercado.
- perfil recém-criado
- poucas informações
- comentários estranhos
- pressão para pagar



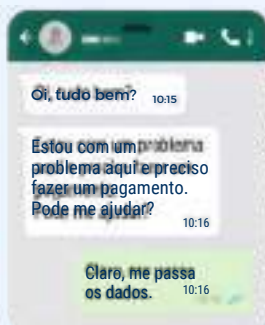
Ação:

crie um checklist com 10 perguntas.

DIA 2



Golpe do WhatsApp



pedido inesperado de dinheiro. Confirme por ligação, outro canal ou pergunta pessoal. Ative a verificação em duas etapas e nunca compartilhe códigos.



Ação:

Pedido urgente de dinheiro = eu sempre confirmo por ligação.

DIA 3



Falsa central do banco



desligue, abra o aplicativo oficial e procure o telefone por conta própria. Nunca forneça senha, código de SMS, código do aplicativo, dados do cartão ou informações bancárias por telefone.



Ação:

salve o telefone oficial do banco.



Dias 4 a 6: confira o Pix e desconfie dos links



DIA
4

Golpe do Pix:

antes de confirmar, confira
nome do destinatário,
banco, valor e motivo.

Em caso de golpe, procure o banco
imediatamente e solicite o MED; registre
também um boletim de ocorrência.

Ação: Nome → banco → valor →
motivo → só então confirmar.

Confirme seu Pix

	Nome	João da Silva
	Banco	Banco do Brasil
	Valor	R\$ 350,00
	Motivo	Pagamento de serviço

Confirmar Pix

DIA
5

Recebi um Pix por engano:

não faça um novo Pix.
Use a função **Devolver**
da própria transação e
guarde provas da situação.

Detalhes da transação

	R\$ 250,00	+ R\$ 250,00
	R\$ Maria Gouas	R\$ 10,15

Devolver

Salvar comprovante

DIA
6

Phishing:

antes de clicar, pergunte:

- Quem enviou?
- Eu esperava isso?
- Para onde o link vai?
- Estão tentando me assustar?
- Posso acessar pelo
aplicativo oficial?

Ação: apague → mensagens
suspeitas, bloqueie remetentes e
atualize aplicativos importantes.

Oferta imperdível!

Clique aqui e ganhe
um prêmio agora.
<http://bit.ly/premio123>

PARE!

Não clique
em links
suspeitos.

A devolução de um Pix recebido por engano deve ser
feita pela própria transação, não por um novo Pix.



Dias 7 a 10: proteja pagamentos, cartões e celular



DIA 7

Boleto falso e QR Code

BOLETO

VENCIMENTO
15/12/2025

VOROR
R\$ 350,00

BENEFICIÁRIO
EMPRESA XYZ LTDA



confira beneficiário, valor e vencimento; um QR Code pode representar um Pix.



Ação: pratique a conferência dos dados de uma conta real sem iniciar uma operação desnecessária.

DIA 8

Falso investimento



desconfie de lucro fácil, rendimento garantido, pressão e supostos especialistas. Verifique quem oferece, se a empresa existe, a documentação, os riscos e os canais oficiais.



Ação: preencha uma Ficha de Verificação de Investimento.

DIA 9

Troca de cartão e maquininha



confira o valor na tela, proteja sua senha, não perca o cartão de vista e confira o cartão ao recebê-lo.



Ação: Eu confiro o valor, digito minha senha protegido e confiro meu cartão antes de sair.

DIA 10

Celular roubado, conta invadidas e mão fantasma



- ✓ use bloqueio de tela e biometria
- ✓ mantenha tudo atualizado
- ✓ não instale aplicativos desconhecidos e nunca entregue acesso remoto.



Se for roubado: bloqueie aparelho, contate a operadora e os bancos, bloqueie cartões, altere senhas, registre ocorrência e monitore movimentações.



Bônus: caí no golpe. E agora?



Pare de conversar. Não envie mais dinheiro.



Contate o banco imediatamente. Solicite contestação ou devolução quando aplicável.



Guarde prints, comprovantes, números e mensagens.



Registre boletim de ocorrência.



No Pix, peça orientação sobre o MED o mais rápido possível.



CARTÃO DE EMERGÊNCIA



PARE



NÃO PAGUE



NÃO CLIQUE



NÃO PASSE CÓDIGOS



FALE COM O BANCO



GUARDE AS PROVAS



CHECKLIST



É golpe?



Estão me pressionando?



Estão pedindo senha ou código?



Estão pedindo Pix?



O preço está estranho?

O link é desconhecido?

Posso confirmar por outro canal?

QUIZ

Uma mensagem pede código recebido por SMS. A resposta correta é desligar e procurar o banco pelo canal oficial.

Texto do seu parágrafo

5 regras pessoais

1.

2.

3.

4.

5.

Pare → Pense → Confira →
Só depois pague.

Recorte o cartão de emergência e mantenha com você!

Este material é educativo e não substitui a orientação do seu banco, das autoridades competentes ou de profissionais especializados.

PROTEÇÃO CONSCIENTE
COM UM HÁBITO



Introdução e Dia 1 — Falsa venda



Golpistas muitas vezes convencem a pessoa a entregar voluntariamente senha, código, informação ou dinheiro.

Regra de ouro:
Parê. Desconfie.
Confira. Só depois decida.



Método dos 10 dias



Entender o golpe



Reconhecer sinais



Saber o que fazer



Praticar o exercício



Falsa venda

Lojas, perfis e anúncios falsos são criados para receber pagamentos por produtos inexistentes.



Sinais de alerta



Preço muito abaixo do mercado



Perfil recém-criado



Poucas informações



Comentários estranhos ou inexistentes



Pressão para pagar imediatamente



Antes de comprar



Procure a empresa em canais oficiais



Confira o endereço (URL) do site



Pesquise reclamações de outros consumidores



Verifique o nome do recebedor do pagamento



Desconfie de links recebidos por mensagem



Ação do dia:

Criar um Checklist Antes de Comprar com 10 perguntas.





Dias 2 e 3 — WhatsApp e falsa central do banco



WhatsApp: golpe do amigo ou familiar

O criminoso se passa por amigo ou familiar e pede dinheiro.



Como confirmar a identidade



Ligue para a pessoa.



Use outro meio de contato.



Faça uma pergunta que somente ela saberia responder.



Nunca transfira dinheiro apenas porque alguém está com pressa.



Proteja sua conta



Ative a verificação em duas etapas.



Mantenha seu celular protegido com senha ou biometria.



Nunca compartilhe códigos de confirmação.



REGRA PESSOAL:

Pedido urgente de dinheiro = eu sempre confirmo por ligação.



Falsa central bancária

O criminoso se apresenta como funcionário e usa frases como:



“Sua conta foi invadida”



“Precisamos cancelar uma transferência”



“Faça um teste”

“Passe o código recebido”

“Instale este aplicativo”

A regra é clara:

Nunca forneça senha, código de SMS, código do aplicativo, dados do cartão ou informações bancárias por telefone.

Como verificar:

Desligue o telefone.

Abra o aplicativo oficial do banco.

Procure o telefone oficial no site ou no app.

Entre em contato por conta própria.



AÇÃO DO DIA:

Salve o telefone oficial do seu banco.



Dias 4 e 5 — Golpe do Pix e Pix recebido por engano



GOLPE DO PIX



Antes de apertar Confirmar, conferir nome do destinatário, banco, valor e motivo.



Nunca confiar somente no nome ou foto do perfil.



Desconfiar de pedidos urgentes.



EM CASO DE GOLPE

Procurar o banco imediatamente para relatar e solicitar o MED e registrar boletim de ocorrência.



Nome → banco → valor → motivo → só então confirmar.

PIX RECEBIDO POR ENGANO

Não devolver fazendo outro Pix.

Usar a função “Devolver” da própria transação.

Guardar prints, comprovantes e mensagens.



NOTA EDUCATIVA

A devolução pela própria transação ajuda a evitar o risco de devolver o dinheiro e depois também ocorrer uma solicitação de devolução da transação original.

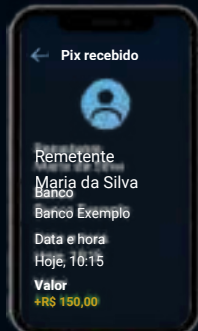
PASSO A PASSO: COMO DEVOLVER UM PIX RECEBIDO POR ENGANO

1 Abrir a transação



Acesse sua área de atividade e toque no Pix recebido.

2 Conferir o remittente



Confira nome, banco, data, hora e valor para ter certeza.

3 Selecionar Devolver



Toque em “Devolver” e siga as instruções na tela.

4 Guardar a prova

Guarde prints, comprovantes e mensagens.



Dias 6 e 7 – Phishing, boleto falso e QR Code



ROTEIRO SOBRE PHISHING



SMS falso

Mensagens com links para supostos bloqueios, prêmios ou cobranças.



E-mail falso

E-mails que imitam empresas e pedem para clicar em links ou informar dados.



WhatsApp falso

Contatos se passando por empresas ou pessoas conhecidas para pedir dinheiro ou dados.



Sites que imitam empresas reais

Páginas falsas que copiam o visual de sites legítimos para roubar seus dados.



REGRA DOS 5 SEGUNDOS

1. Quem enviou?
2. Eu estava esperando isso?
3. Para onde esse link vai?
4. Estão tentando me assustar?
5. Posso acessar o serviço pelo aplicativo oficial?



AÇÃO DO DIA



Apagar mensagens suspeitas.
Blockar remetentes.
Excluir links desconhecidos.
Atualizar aplicativos importantes.



BOLETO FALSO E QR CODE



Confira sempre o beneficiário, valor e vencimento.



Desconfie de boletos recebidos inesperadamente.



Lembre-se, um QR Code em um documento pode representar um Pix e não funciona como um boleto tradicional.



AÇÃO DO DIA

Escolher uma conta real e praticar a conferência dos dados sem efetuar uma nova operação desnecessária.



Dias 8 a 10 — Investimento, cartão e celular



1. FALSO INVESTIMENTO

Desconfie sempre deste roteiro:

- Lucro fácil e rendimento garantido
- Pressão para investir rapidamente
- Supostos especialistas "renomados"
- Depoimentos e provas manipuladas



**Ação: Preencha a
Ficha de Verificação
de Investimento.**

Perguntas obrigatórias:

- 1. Quem oferece?
- 2. A empresa existe?
- 3. Como funciona?
- 4. Existe documentação?
- 5. O risco foi explicado?
- 6. Posso verificar a instituição por canais oficiais?



2. TROCA DE CARTÃO E MAQUININHA

- Pague presencialmente com atenção
- Nunca entregue sua senha
- Não deixe o cartão desaparecer de vista
- Confira seu cartão ao recebê-lo
- Confira o valor na maquininha



Regra de ouro:

Eu confiro o valor na tela, digito minha senha protegido e confiro meu cartão antes de sair.



3. SEGURANÇA DO CELULAR

- Use bloqueio de tela e biometria
- Instale apenas aplicativos confiáveis
- Mantenha o sistema e apps atualizados
- Nunca entregue acesso remoto ao seu celular



4. EM CASO DE ROUBO OU PERDA

- Bloqueie o aparelho
- Contate sua operadora
- Contate seus bancos e financeiras
- Bloqueie cartões
- Altere suas senhas
- Registre ocorrência na polícia
- Monitore suas movimentações

12

Bônus, desafio final e conclusão



SEQUÊNCIA DE EMERGÊNCIA

- 1 Pare de conversar com o golpista.
- 2 Não envie mais dinheiro.
- 3 Entre imediatamente em contato com o banco.
- 4 Solicite contestação/devolução quando aplicável.
- 5 Guarde prints, comprovantes, números e mensagens.
- 6 Registre boletim de ocorrência.



PARE



NÃO PAGUE



NÃO CLIQUE



NÃO PASSE CÓDIGOS



FALE COM O BANCO



GUARDE AS PROVAS



CHECKLIST É GOLPE:

- ☐ estão me pressionando?
- ☐ estão pedindo senha?
- ☐ estão pedindo código?
- ☐ estão pedindo Pix?
- ☐ o preço está estranho?
- ☐ o link é desconhecido?
- ☐ a pessoa diz ser alguém que conheço?
- ☐ posso confirmar por outro canal?



MEU PLANO ANTIGOLPE

- 1 _____
- 2 _____
- 3 _____
- 4 _____
- 5 _____



REGRA PARA PAGAMENTOS

Nunca faço um pagamento quando estou com medo, pressa ou pressão. Primeiro para e verifico.



REGRA PARA MENSAGENS

Mensagem inesperada + urgência + pedido de dinheiro/dados = verificar por outro canal.

Pare se

Confira

Só depois pague.

a partir de hoje, eu nunca mais vou: _____

antes de fazer um Pix, eu sempre vou: _____

se alguém me pressionar, eu vou: _____

meu maior aprendizado foi: _____

meu próximo passo será: _____



Procure sempre seu banco e as autoridades pelos canais oficiais.
Desconfie de contatos que chegam até você.

Vá ao banco, disque números oficiais e registre ocorrências.

