



DATASPECTRE
SAFE

GUIA ANTI-GOLPES

**PARA QUEM USA O CELULAR
COM POUCA FAMILIARIDADE**

Aprenda a reconhecer mensagens, ligações, links e pedidos suspeitos antes de clicar, pagar ou informar seus dados.

Leitura simples • letras grandes • exemplos práticos

DataSpectre Safe

CAPÍTULO 0

COMECE POR AQUI

Este guia foi feito para ser lido devagar, sem termos difíceis.

Você não precisa entender de tecnologia para se proteger.

Golpes digitais funcionam porque tentam fazer a pessoa agir com pressa, medo, vergonha, curiosidade ou esperança. O objetivo deste guia é ensinar uma rotina simples: parar, conferir e só depois agir.

IMPORTANTE

Os casos deste guia são exemplos educativos inspirados em golpes comuns. Nomes, números e situações pessoais foram adaptados ou inventados. Nunca use este material como garantia de que uma mensagem ou site é seguro. Em caso de dúvida, confirme pelo canal oficial.

Como usar este guia

1. Leia um capítulo por vez. Não precisa terminar tudo no mesmo dia.
2. Mostre as páginas importantes para alguém de confiança da família.
3. Antes de clicar, pagar ou passar código, volte às “Regras simples”.
4. Se já caiu em um golpe, vá direto ao capítulo “Fui vítima: o que fazer agora”.

A FRASE MAIS IMPORTANTE

SE ALGUÉM ESTÁ APRESSANDO VOCÊ, NÃO DECIDA NA PRESSA.

CAPÍTULO

SUMÁRIO

Use esta lista como mapa do guia.

- 
1. Conhecendo o celular sem medo
 2. As 8 bandeiras vermelhas de um golpe
 3. Golpes no WhatsApp e mensagens
 4. Ligações falsas de banco e suporte
 5. PIX: como evitar perder dinheiro
 6. Boletos, QR Codes e cobranças falsas
 7. Compras online, lojas e marketplaces
 8. Redes sociais, romance e investimento
 9. Entregas, benefícios e falsas vagas
 10. Links, SMS e e-mails falsos

SUMÁRIO - CONTINUAÇÃO

11. Golpes com voz, vídeo e inteligência artificial
12. Senhas e proteção das contas
13. Configurações simples que aumentam sua segurança
14. Celular perdido ou roubado
15. Fui vítima: o que fazer agora
16. Plano de proteção da família
17. SafeCheck: antes de clicar, pagar ou responder
18. Exercícios e situações para treinar
19. Glossário simples
20. Checklist final para imprimir ou salvar

CAPÍTULO 1

CONHECENDO O CELULAR SEM MEDO

O básico que ajuda você a não cair em armadilhas.

Três coisas que você precisa reconhecer

APLICATIVO

É o programa que você abre no celular: WhatsApp, banco, Instagram, câmera e outros. Instale aplicativos somente pela loja oficial do aparelho.

LINK

É um endereço que abre uma página na internet. Pode chegar por mensagem, SMS, e-mail ou rede social. Um link pode ser verdadeiro ou falso.

CÓDIGO DE CONFIRMAÇÃO

É um número temporário usado para provar que é você. Nunca entregue esse código a quem pediu por mensagem ou ligação.

Não tenha vergonha de perguntar

Golpistas gostam de fazer a vítima sentir que precisa resolver tudo sozinha. Se algo parece estranho, peça ajuda a uma pessoa de confiança antes de tocar em qualquer botão.

REGRA SIMPLES

PARAR É UMA AÇÃO DE SEGURANÇA.

Fechar uma mensagem, desligar uma ligação ou deixar uma compra para depois não causa prejuízo. Agir com pressa pode causar.

Quando o celular “pede” alguma coisa

- Leia a tela antes de tocar em “Permitir”, “Continuar” ou “Confirmar”.
- Se não entende o pedido, não aceite automaticamente.
- Banco verdadeiro não precisa que um desconhecido controle a tela do seu celular.
- Desconfie de quem manda instalar aplicativo durante uma ligação.

CAPÍTULO 2

AS 8 BANDEIRAS VERMELHAS

Um golpe geralmente mostra vários destes sinais ao mesmo tempo.

1. PRESSA

“É agora”, “última chance”, “sua conta será bloqueada”.

2. MEDO

“Seu cartão foi clonado”, “há uma compra suspeita”, “você tem uma dívida urgente”.

3. SEGREDO

“Não conte para ninguém”, “não desligue a ligação”.

4. DINHEIRO

Pedido de PIX, transferência, boleto ou pagamento inesperado.

5. CÓDIGO

Pedido de código recebido por SMS, WhatsApp, e-mail ou aplicativo.

6. LINK

Mandam clicar para “confirmar”, “cancelar”, “receber” ou “verificar”.

7. INSTALAÇÃO

Pedem para instalar aplicativo, compartilhar tela ou dar acesso remoto.

8. BOM DEMAIS

Prêmio, investimento com lucro garantido, produto muito barato ou emprego fácil demais.

SE APARECEREM DUAS OU MAIS BANDEIRAS

Pare. Não clique, não pague e não informe dados. Confirme por outro caminho.

CAPÍTULO 3

GOLPES NO WHATSAPP E MENSAGENS

O golpista tenta parecer alguém conhecido ou uma empresa confiável.

Golpe do “número novo”

EXEMPLO DE MENSAGEM SUSPEITA

“Oi mãe, meu celular quebrou.”

“Esse é meu número novo.”

“Preciso pagar uma conta agora. Você consegue fazer um PIX?”

REGRA SIMPLES

NÚMERO NOVO + PEDIDO DE DINHEIRO =
CONFIRME POR LIGAÇÃO.

Ligue para o número antigo ou fale com a pessoa por outro meio. Faça uma pergunta que só ela saberia responder.

Caso 1 - O filho com “celular quebrado”

CASO PRÁTICO - NOMES FICTÍCIOS

Dona Helena, 71 anos: recebe uma mensagem com a foto do filho e um novo número. A pessoa pede R\$ 1.200 para uma conta de terceiro e diz que está sem acesso ao banco.

SINAL DE PERIGO

Foto e jeito de escrever não provam identidade. O pedido de urgência e a conta de terceiro aumentam o risco.

COMO SE PROTEGER

Antes de pagar, Dona Helena deve ligar para o filho no número antigo ou para outro familiar. Se não conseguir confirmar, não faz o PIX.

Golpe do código do WhatsApp

O criminoso tenta registrar sua conta em outro aparelho. Para isso, precisa do código que chega no seu celular. Ele inventa uma história para fazer você entregar esse código.

EXEMPLO DE MENSAGEM SUSPEITA

“Sou do suporte.”

“Enviei um código para confirmar seu cadastro.”

“Me passe os 6 números que chegaram por SMS.”

NUNCA FAÇA ISTO

Nunca ditar código de verificação para outra pessoa, mesmo que ela use logo, foto ou nome de empresa.

Perfil copiado

Às vezes o criminoso não invade a conta: apenas copia foto e nome e cria outro número. Por isso, reconhecer a foto não é suficiente.

CAPÍTULO 4

LIGAÇÕES FALSAS DE BANCO E SUPORTE

Desligar e ligar você mesmo é uma das melhores defesas.

EXEMPLO DE MENSAGEM SUSPEITA

“Sou da central de segurança.”

“Detectamos uma compra de alto valor.”

“Não desligue. Vou transferir para o setor de fraude.”

O golpista pode saber seu nome, parte do CPF ou o nome do banco. Isso não prova que a ligação é verdadeira.

SINAIS MUITO PERIGOSOS

A pessoa pede senha, código, PIX “de segurança”, instalação de aplicativo, compartilhamento de tela, envio do cartão ou transferência para “conta protegida”.

REGRA SIMPLES

DESLIGUE E LIGUE VOCÊ MESMO.

Use o telefone que aparece atrás do cartão, dentro do aplicativo oficial ou no site oficial digitado por você. Não use o número que a pessoa acabou de mandar.

Caso 2 - A falsa central do banco

CASO PRÁTICO - NOMES FICTÍCIOS

Seu Antônio, 67 anos: recebe uma ligação dizendo que houve uma compra de R\$ 4.800. O atendente manda instalar um aplicativo para “cancelar a compra”.

SINAL DE PERIGO

Instalar aplicativo durante uma ligação pode permitir que o criminoso veja ou controle a tela.

COMO SE PROTEGER

Seu Antônio deve encerrar a ligação. Depois, abre o aplicativo do banco sozinho ou liga para o número oficial e pergunta se existe alguma ocorrência.

CAPÍTULO 5

PIX: COMO EVITAR PERDER DINHEIRO

PIX é rápido. A sua conferência também precisa acontecer antes de confirmar.



Antes de apertar “Confirmar”

1. Leia o nome de quem vai receber.
2. Confira o valor.
3. Pergunte por que o pagamento está sendo pedido.
4. Se a pessoa mudou de número, confirme por outro caminho.
5. Se houver pressão, saia da tela e confirme com calma.

ATENÇÃO AO NOME DO RECEBEDOR

Se você está pagando “seu filho” e aparece o nome de uma pessoa desconhecida, não trate isso como normal. Pare e confirme.

Se você fez PIX para um golpista

Entre em contato com o banco o mais rápido possível e informe que foi vítima de fraude. O Banco Central orienta solicitar a devolução pelo Mecanismo Especial de Devolução (MED) quando o caso se enquadrar nas regras do mecanismo.

MED NÃO É GARANTIA DE RECUPERAÇÃO

O MED aumenta a chance de bloqueio e devolução em fraudes, mas a devolução pode ser parcial ou não acontecer se não houver recursos disponíveis ou se o caso não se enquadrar.

PRAZO OFICIAL

Segundo o Banco Central, o pedido de devolução pelo MED pode ser registrado na instituição em até 80 dias da data do PIX em caso de fraude, golpe ou crime. Mesmo assim, agir imediatamente é muito melhor.

Golpe do “PIX por engano”

Se alguém disser que fez um PIX por engano para você, confira primeiro o seu extrato. Se o valor realmente entrou e você decidir devolver, use a função “Devolver” da própria transação. Não faça um novo PIX para uma conta diferente.

CAPÍTULO 6

BOLETOS, QR CODES E COBRANÇAS FALSAS

Não confie somente na aparência do documento.

Boleto falso

O boleto pode ter logotipo e aparência correta, mas os dados de pagamento podem ter sido alterados.

- Confira o nome do beneficiário antes de pagar.
- Desconfie de boleto recebido de forma inesperada por WhatsApp.
- Se for cobrança de empresa conhecida, abra o aplicativo ou site oficial e gere a cobrança por lá.
- Se o valor ou nome estiver diferente, pare.

QR Code falso

QR Code é apenas uma forma de abrir um endereço ou pagamento. Ele não é automaticamente seguro.

ANTES DE PAGAR

Depois de ler o QR Code, confira na tela do banco o nome do recebedor e o valor. Só confirme quando tudo estiver correto.

Caso 3 - A conta de energia “atrasada”

CASO PRÁTICO - NOMES FICTÍCIOS

Dona Célia, 73 anos: recebe um boleto por mensagem dizendo que a energia será cortada naquele dia. O documento parece verdadeiro, mas o beneficiário é desconhecido.

SINAL DE PERIGO

Ameaça de corte imediato + cobrança inesperada + beneficiário diferente.

COMO SE PROTEGER

Ela deve entrar no aplicativo/site oficial da empresa ou ligar para o atendimento oficial antes de pagar.

CAPÍTULO 7

COMPRAS ONLINE, LOJAS E MARKETPLACES

Preço baixo não compensa perder dinheiro ou dados.

Loja falsa

- Desconfie de preços muito abaixo dos concorrentes.
- Procure o nome da loja fora do anúncio.
- Veja se o endereço do site está escrito corretamente.
- Prefira meios de pagamento com proteção ao comprador quando disponíveis.
- Evite sair do aplicativo de marketplace para negociar por WhatsApp se isso eliminar as proteções da plataforma.

ANÚNCIO EM REDE SOCIAL NÃO É SELO DE CONFIANÇA

Criminosos também podem comprar anúncios. O fato de aparecer como publicidade não prova que a loja é verdadeira.

O golpe da “taxa para liberar produto”

Depois de uma compra ou falsa compra, podem surgir cobranças de taxa, seguro, frete adicional ou liberação alfandegária. Não pague só porque a mensagem parece relacionada a algo que você comprou.

REGRA SIMPLES

VOLTE AO APLICATIVO OFICIAL.

Se comprou em uma plataforma, confira o pedido dentro dela. Não resolva cobrança inesperada pelo link que chegou por mensagem.

CAPÍTULO 8

REDES SOCIAIS, ROMANCE E INVESTIMENTOS

Golpes também usam confiança, carinho e promessa de lucro.



Golpe do romance

A pessoa cria vínculo emocional e depois aparece uma emergência: passagem, hospital, encomenda presa, dívida ou documento. O pedido de dinheiro pode começar pequeno e aumentar.

SINAIS COMUNS

Evita vídeo ao vivo, sempre tem desculpa para não encontrar, histórias dramáticas frequentes, pedidos de dinheiro e pressão para manter segredo.

Investimento com lucro garantido

Nenhum investimento sério precisa prometer dinheiro fácil e sem risco. Golpistas mostram prints, depoimentos e supostos saldos que podem ser falsos.

FRASES PERIGOSAS

“Lucro garantido”, “dobrar em poucos dias”,
“oportunidade secreta”, “só hoje”, “mande PIX para
ativar a conta”.

Caso 4 - O “especialista” da internet

CASO PRÁTICO - NOMES FICTÍCIOS

Sr. Paulo, 64 anos: vê um perfil que promete
rendimento de 5% ao dia. Depois do primeiro depósito,
o site mostra lucro. Para sacar, pedem uma nova
“taxa”.

SINAL DE PERIGO

O saldo na tela pode ser apenas um número falso.
Pedir pagamento para liberar saque é um sinal grave.

COMO SE PROTEGER

Não envie mais dinheiro. Preserve provas, fale com o
banco e registre a ocorrência se houver prejuízo.

CAPÍTULO 9

ENTREGAS, BENEFÍCIOS E FALSAS VAGAS

Golpistas gostam de assuntos que chamam atenção no dia a dia.

Entrega pendente

EXEMPLO DE MENSAGEM SUSPEITA

“Seu pacote está retido.”

“Pague R\$ 4,97 para liberar a entrega.”

“Acesse: link-exemplo...”

COMO CONFERIR

Abra o aplicativo ou site oficial da loja/transportadora digitando você mesmo. Não use o link da mensagem.

Benefício, INSS, gov.br ou restituição

Mensagens podem prometer valor liberado, atualização cadastral ou bloqueio de benefício. Não

informe senha da conta gov.br e não passe código de acesso para ninguém.

CONTA GOV.BR

A senha deve ser tratada com o mesmo cuidado da senha do banco. A verificação em duas etapas aumenta a proteção e o código é gerado dentro do aplicativo gov.br.

Falsa vaga de emprego

- Desconfie de vaga que exige pagamento para começar.
- Não pague “taxa de material”, “curso obrigatório” ou “liberação de cadastro” sem verificar a empresa.
- Cuidado com promessa de salário alto para tarefa muito simples.
- Não envie foto de documentos para desconhecidos sem confirmar a necessidade e a empresa.

CAPÍTULO 10

LINKS, SMS E E-MAILS FALSOS

Você não precisa abrir um link para descobrir se a mensagem faz sentido.

Phishing em linguagem simples

Phishing é uma tentativa de fazer você entrar em uma página falsa e informar dados como senha, CPF, cartão ou código.

PENSE ANTES DE ABRIR

Eu estava esperando esta mensagem? Conheço o remetente? Preciso mesmo clicar? Posso abrir o aplicativo oficial sem usar o link?

Endereço parecido não é endereço igual

Golpistas usam nomes muito parecidos com bancos, lojas e serviços. Uma letra trocada já pode levar para outro site.

EXEMPLO DE MENSAGEM SUSPEITA

VERDADEIRO (exemplo): empresa.com.br

SUSPEITO: empresa-seguranca-login.xyz

SUSPEITO: empresa.com.br.pagina-falsa.example

NÃO TENHA “TESTAR” LINK ESTRANHO

Se o link parece suspeito, não clique para ver o que acontece. A forma mais segura é entrar no serviço pelo aplicativo oficial ou digitar o endereço que você já conhece.

CAPÍTULO 11

GOLPES COM VOZ, VÍDEO E INTELIGÊNCIA ARTIFICIAL

Ouvir a voz de alguém conhecido já não é prova suficiente.

Ferramentas de inteligência artificial conseguem imitar voz e criar imagens ou vídeos falsos. O criminoso pode usar isso para tornar um pedido urgente mais convincente.

PROTEÇÃO SIMPLES DA FAMÍLIA

Escolham uma palavra ou pergunta secreta que não apareça nas redes sociais. Em pedido urgente de dinheiro, use essa confirmação e ligue para a pessoa por um número conhecido.

Caso 5 - A voz do neto

CASO PRÁTICO - NOMES FICTÍCIOS

Dona Marta, 76 anos: recebe uma ligação com uma voz parecida com a do neto dizendo que sofreu um acidente e precisa de dinheiro. Outra pessoa pega o telefone e passa os dados para o pagamento.

SINAL DE PERIGO

Pressa, emoção forte e pedido de dinheiro. A voz pode ser imitada ou gravada.

COMO SE PROTEGER

Dona Marta deve desligar e ligar diretamente para o neto ou para os pais dele. Não deve continuar presa à ligação do desconhecido.

REGRA SIMPLES

VOZ, FOTO E VÍDEO PODEM SER FALSIFICADOS.

A melhor prova é confirmar por outro canal e usar uma informação combinada previamente com a família.

CAPÍTULO 12

SENHAS E PROTEÇÃO DAS CONTAS

Uma boa senha reduz o estrago quando um serviço é atacado.



O que evitar

- Usar a mesma senha no banco, e-mail e redes sociais.
- Usar nome, data de nascimento ou “123456”.
- Enviar senha por WhatsApp.
- Anotar senha em mensagem para você mesmo sem proteção.

Uma forma simples de criar senha forte

Use uma frase longa que faça sentido só para você e misture palavras. Exemplo didático:

“CafeNaVarandaTodaManha!” Não copie este exemplo; crie o seu.

PRIORIDADE NÚMERO 1: PROTEJA O E-MAIL

Seu e-mail costuma ser usado para recuperar outras contas. Se alguém entra nele, pode tentar redefinir senhas de vários serviços.

Verificação em duas etapas (2FA)

É uma segunda confirmação além da senha. Ative principalmente no e-mail, WhatsApp, redes sociais e conta gov.br quando disponível.

NUNCA COMPARTILHE O SEGUNDO FATOR

Código de verificação serve para provar que é você. Se outra pessoa pede esse código, ela pode estar tentando entrar na sua conta.

CAPÍTULO 13

CONFIGURAÇÕES SIMPLES QUE AUMENTAM SUA SEGURANÇA

Peça ajuda a alguém de confiança para configurar uma vez e deixar funcionando.



BLOQUEIO DE TELA

Use PIN, senha, digital ou reconhecimento facial. Evite deixar o aparelho sem bloqueio.

ATUALIZAÇÕES

Mantenha o sistema e os aplicativos atualizados. Atualizações corrigem falhas de segurança.

LOJA OFICIAL

Instale aplicativos pela Google Play ou App Store. Evite arquivos enviados por WhatsApp.

PERMISSÕES

Aplicativo de lanterna, por exemplo, não precisa controlar suas mensagens. Revise permissões estranhas.

NOTIFICAÇÕES NA TELA BLOQUEADA

Se possível, esconda o conteúdo de códigos e mensagens sensíveis quando a tela estiver bloqueada.

BACKUP

Mantenha fotos e contatos importantes em backup para reduzir o prejuízo se o aparelho for perdido.

BIOMETRIA NO BANCO

Quando o aplicativo permitir, use biometria junto com senha/PIN.

CELULAR SEGURO

No Brasil, o programa Celular Seguro permite registrar alerta e acionar bloqueios junto a participantes em caso de roubo ou furto.

CAPÍTULO 14

CELULAR PERDIDO OU ROUBADO

A velocidade das primeiras ações pode reduzir o prejuízo.

Se o aparelho sumiu

- 1.** Use outro aparelho para tentar localizar ou bloquear o celular pelos recursos do sistema, se você já os tinha configurado.
- 2.** Comunique a operadora e solicite bloqueio da linha quando necessário.
- 3.** Use o Celular Seguro, se você já estiver cadastrado ou tiver acesso à plataforma e o caso se enquadrar.
- 4.** Avise os bancos e proteja os aplicativos financeiros.
- 5.** Troque primeiro a senha do e-mail principal e depois das contas mais importantes.
- 6.** Registre boletim de ocorrência em caso de roubo ou furto.

7. Avise familiares para ignorarem pedidos de dinheiro feitos em seu nome.

ORIENTAÇÃO DA ANATEL

Em caso de perda ou roubo, a Anatel orienta comunicar a prestadora e solicitar o bloqueio do serviço. Em roubo ou furto, registre a ocorrência policial.

PREPARE ANTES

Cadastre uma pessoa de confiança no Celular Seguro e anote, em local seguro fora do celular, os contatos oficiais do banco e da operadora.

CAPÍTULO 15

FUI VÍTIMA: O QUE FAZER AGORA

Não esconda por vergonha. Quanto antes você agir, melhor.

PRIMEIRA REGRA

PARE DE FALAR COM O GOLPISTA. Não envie mais dinheiro para “recuperar” o que perdeu.

Se houve PIX ou transferência

- 1.** Fale imediatamente com o banco pelo aplicativo, telefone oficial ou agência.
- 2.** Informe que foi vítima de fraude/golpe e pergunte sobre o procedimento aplicável, incluindo MED no caso de PIX quando cabível.
- 3.** Guarde comprovantes, chaves PIX, nomes, números e conversas.
- 4.** Registre boletim de ocorrência.
- 5.** Se necessário, registre reclamações nos canais oficiais competentes.

Se informou senha ou código

1. Troque a senha imediatamente por um aparelho confiável.
2. Comece pelo e-mail principal.
3. Encerre sessões ou dispositivos desconhecidos, se o serviço oferecer essa opção.
4. Ative verificação em duas etapas.
5. Avise banco e serviços afetados quando houver risco financeiro.

Se instalou aplicativo indicado por desconhecido

1. Desconecte o aparelho da internet se perceber controle estranho ou operações acontecendo sem você.
2. Use outro aparelho confiável para falar com o banco e trocar senhas importantes.
3. Procure ajuda técnica de confiança para remover o aplicativo e revisar o aparelho.
4. Não faça operações bancárias no aparelho até ter certeza de que está seguro.

CUIDADO COM O “GOLPE DA RECUPERAÇÃO”

Depois de um golpe, outra pessoa pode prometer recuperar seu dinheiro mediante pagamento. Não envie mais dinheiro para desconhecidos.

O que guardar como prova

- Prints das conversas e mensagens.
- Número de telefone, perfil e nome usado pelo golpista.
- Links e endereços de sites recebidos.
- Comprovantes de PIX, transferências ou boletos.
- Horário aproximado das ligações e o que foi pedido.
- Não apague tudo antes de registrar as informações importantes.

NÃO SE ARRISQUE PARA CONSEGUIR PROVA

Não continue conversando com o golpista só para tentar obter mais informações. Preserve o que você já tem e interrompa o contato.

CAPÍTULO 16

PLANO DE PROTEÇÃO DA FAMÍLIA

Uma família organizada é mais difícil de enganar.

Combine hoje

1. Uma palavra secreta para pedidos de emergência.
2. Quem deve ser chamado quando houver dúvida.
3. Que ninguém da família pede PIX urgente sem confirmação por ligação.
4. Que códigos de SMS e senhas nunca são compartilhados.
5. Que todos podem desligar uma ligação suspeita sem medo de parecer mal-educados.

FRASE PRONTA PARA USAR

“Eu não vou resolver isso por esta ligação. Vou desligar e entrar em contato pelo número oficial.”

Ajude sem tirar a autonomia

Para ajudar um idoso ou iniciante, configure junto, explique devagar e deixe um papel com três contatos confiáveis. O objetivo é dar segurança para a pessoa decidir melhor, não fazer tudo por ela.

Cartão de emergência da família

Preencha e deixe perto do carregador ou em outro local fácil de encontrar:

CONTATO 1

Nome: _____ Telefone: _____

CONTATO 2

Nome: _____ Telefone: _____

BANCO / OPERADORA

Anote somente o telefone oficial. Nunca anote senha ou código neste papel.

CAPÍTULO 17

SAFECHECK

Use estas perguntas antes de clicar, pagar ou responder.

Antes de clicar em um link

PERGUNTE A SI MESMO

Eu esperava esta mensagem?

PERGUNTE A SI MESMO

O remetente é realmente conhecido?

PERGUNTE A SI MESMO

A mensagem me ameaça ou me apressa?

PERGUNTE A SI MESMO

Posso abrir o aplicativo oficial em vez do link?

PERGUNTE A SI MESMO

O endereço parece estranho ou diferente?

SE TIVER DÚVIDA EM UMA PERGUNTA

Não clique. Entre no serviço por conta própria ou peça ajuda.

Antes de fazer PIX

PERGUNTE A SI MESMO

Eu confirmei a identidade da pessoa por outro canal?

PERGUNTE A SI MESMO

O nome do recebedor faz sentido?

PERGUNTE A SI MESMO

Existe urgência exagerada?

PERGUNTE A SI MESMO

A pessoa pediu segredo?

PERGUNTE A SI MESMO

O dinheiro vai para um terceiro desconhecido?

DUAS RESPOSTAS PREOCUPANTES

Trate como alto risco até confirmar.

Antes de passar um código

RESPOSTA PADRÃO

Não passe. Código de confirmação é para você usar no seu próprio aparelho.

CAPÍTULO 18

TREINE COM SITUAÇÕES

Leia, escolha o que faria e depois veja a resposta.

Situação 1

Seu sobrinho manda mensagem de um número novo e pede PIX.

MELHOR ATITUDE

Ligar para o número antigo ou para outro familiar antes de pagar.

CORRETO: confirme por outro canal.

Situação 2

O banco liga e manda instalar um aplicativo para cancelar uma compra.

MELHOR ATITUDE

Desligar e falar com o banco por canal oficial.

CORRETO: banco não precisa de controle remoto do seu celular para “cancelar” compra.

Situação 3

Chega SMS dizendo que seu pacote está preso e pede R\$ 3,90.

MELHOR ATITUDE

Abrir o aplicativo/site oficial da loja ou transportadora, sem usar o link.

CORRETO: confirme por caminho independente.

Situação 4

Uma pessoa pede o código de seis números que chegou por SMS.

MELHOR ATITUDE

Não informar o código.

CORRETO: esse código pode permitir acesso à sua conta.

Situação 5

Um investimento promete dobrar seu dinheiro em 15 dias.

MELHOR ATITUDE

Não transferir e pesquisar por fontes independentes.

CORRETO: promessa de lucro garantido é sinal de risco.

Situação 6

Você recebeu PIX “por engano” e pedem devolução para outra conta.

MELHOR ATITUDE

Conferir o extrato e usar a função de devolução da própria transação, se for devolver.

CORRETO: não faça novo PIX para conta diferente.

Situação 7

Aparece anúncio de TV por metade do preço e só aceita PIX.

MELHOR ATITUDE

Desconfiar, pesquisar a loja e não pagar até confirmar.

CORRETO: preço irreal + pagamento sem proteção aumenta o risco.

Situação 8

Uma voz parecida com a de um neto pede dinheiro por acidente.

MELHOR ATITUDE

Desligar e ligar para o neto ou familiares em números conhecidos.

CORRETO: voz pode ser imitada.

Situação 9

Você clicou num link, mas não digitou nada.

MELHOR ATITUDE

Fechar a página, não instalar nada e observar se houve download ou pedido de permissão.

CORRETO: não continue interagindo com a página.

Situação 10

Você percebeu que caiu num golpe.

MELHOR ATITUDE

Agir rápido, avisar banco/serviço afetado, guardar provas e registrar ocorrência.

CORRETO: vergonha não ajuda; velocidade ajuda.

CAPÍTULO 19

GLOSSÁRIO SIMPLES

Palavras que aparecem muito quando falamos de segurança digital.

APLICATIVO (APP)

Programa instalado no celular, como WhatsApp ou banco.

BIOMETRIA

Uso da digital ou do rosto para confirmar sua identidade.

CÓDIGO DE VERIFICAÇÃO

Número temporário usado para confirmar acesso. Não compartilhe.

GOLPE

Engano usado para conseguir dinheiro, dados, acesso ou outra vantagem.

LINK

Endereço que abre uma página ou conteúdo na internet.

PHISHING

Mensagem ou página falsa que tenta roubar dados ou senhas.

PIX

Forma de pagamento instantâneo. Antes de confirmar, confira recebedor e valor.

QR CODE

Imagem quadrada que pode abrir link ou pagamento. Confira o destino antes de confirmar.

SENHA

Segredo usado para entrar em uma conta.

2FA / DUAS ETAPAS

Segunda confirmação além da senha.

SUPORTE REMOTO

Ferramenta que permite controlar um aparelho à distância. Não dê acesso a desconhecidos.

DEEPPFAKE

Áudio, imagem ou vídeo manipulado para imitar alguém.

MED

Mecanismo Especial de Devolução do PIX para situações previstas de fraude, golpe ou crime.

CAPÍTULO 20

CHECKLIST FINAL

Salve esta página ou imprima e deixe perto do celular.

- ☐ Não faço PIX urgente sem confirmar a pessoa por outro meio.
- ☐ Não passo código recebido por SMS, WhatsApp, e-mail ou aplicativo.
- ☐ Não instalo aplicativo porque alguém mandou durante uma ligação.
- ☐ Não clico em link inesperado para resolver problema de banco, entrega ou benefício.
- ☐ Confiro o nome do recebedor antes de pagar.
- ☐ Desligo ligações suspeitas e procuro o canal oficial por conta própria.
- ☐ Protejo meu e-mail com senha forte e duas etapas.
- ☐ Mantenho meu celular bloqueado e atualizado.

- ☐ Tenho pelo menos uma pessoa de confiança para pedir ajuda.
- ☐ Se eu cair em golpe, ajo rápido e não escondo por vergonha.

LEMBRE SEMPRE

PARE • CONFIRA • SÓ DEPOIS AJA

CAPÍTULO

FONTES E ATUALIZAÇÃO

Conteúdo educativo baseado em boas práticas e orientações oficiais consultadas em agosto de 2026.

Banco Central do Brasil

PIX, golpes e Mecanismo Especial de Devolução (MED).

<https://www.bcb.gov.br/meubc/faqs/s/pix>

CERT.br / NIC.br

Cartilha de Segurança para Internet e fascículos sobre golpes.

<https://cartilha.cert.br/>

Governo Digital - gov.br

Segurança da conta e verificação em duas etapas.

<https://www.gov.br/governodigital/pt-br/identidade/conta-gov-br/seguranca-da-conta>

Anatel

Orientações para perda ou roubo de aparelho celular.

<https://www.gov.br/anatel/pt-br/consumidor/conheca-seus-direitos-2/telefonica-movel/perda-ou-roubo-do-aparelho-celular>

Ministério da Justiça e Segurança Pública / Anatel

Programa Celular Seguro.

<https://www.gov.br/mj/pt-br/acesso-a-informacao/acoes-e-programas/celular-seguro/programa-celular-seguro>

AVISO

Procedimentos de bancos, aplicativos e órgãos públicos podem mudar. Em caso de dúvida, consulte sempre o aplicativo, site ou telefone oficial atualizado da instituição.

Compartilhe este guia

Muitas vítimas de golpe não são “desatentas”. Elas são colocadas sob pressão por técnicas de manipulação. Compartilhar informação simples e sem julgamento ajuda famílias inteiras a ficarem mais seguras.

DATASPECTRE SAFE

Educação • Prevenção • Análise