

100 GOLPES PARA RECONHECER

Como cada golpe funciona, o sinal de alerta e o que fazer.

Como usar: procure o golpe pela categoria ou pelo número. Todos têm fonte, listada no fim. A versão com busca está em daemon-px-links.vercel.app/golpes/.

Categorias

Bancos e Pix (13)

WhatsApp e redes sociais (12)

Compras e vendas (13)

Trabalho e dinheiro fácil (10)

Governo, justiça e contas da casa (14)

Celular e contas (12)

Na rua e em casa (6)

Família, saúde e emergências (9)

Viagens, prêmios e doações (7)

Ameaças, cripto e contas laranja (4)

1. Falsa central do banco

Como funciona: Alguém liga dizendo ser do banco, fala de uma compra ou fraude na sua conta e pede senha, código ou uma transferência para "proteger" o dinheiro.

Sinal de alerta: Banco pedindo senha, código ou transferência por telefone.

O que fazer: Desligue e ligue você mesmo no número do verso do cartão, de preferência de outro aparelho.

2. Falso motoboy do banco

Como funciona: Depois de uma ligação da falsa central, pedem que você corte o cartão sem danificar o chip e avisam que um motoboy vai buscá-lo.

Sinal de alerta: Banco querendo buscar seu cartão em casa.

O que fazer: Não entregue o cartão a ninguém. Banco não recolhe cartão nem manda portador.

3. SMS de compra suspeita

Como funciona: Chega um SMS ou mensagem sobre uma compra alta no seu cartão, com um 0800 para "cancelar". Quem atende é o golpista.

Sinal de alerta: Mensagem com número de telefone ou link para resolver uma compra que você não fez.

O que fazer: Não ligue para o número da mensagem. Confira no app do banco ou pelo telefone do verso do cartão.

4. Mão fantasma (acesso remoto)

Como funciona: O falso funcionário pede que você instale um app para "verificar" sua conta. O app dá a ele o controle do seu celular.

Sinal de alerta: Alguém que ligou pedindo para instalar um aplicativo.

O que fazer: Nunca instale app a pedido de quem ligou. Banco não pede isso.

5. Boleto adulterado

Como funciona: Um vírus ou um e-mail falso troca o código de barras do boleto. Você paga o valor certo, mas o dinheiro vai para o golpista.

Sinal de alerta: Nome de quem recebe diferente da empresa que cobrou.

O que fazer: Antes de pagar, confira no app o nome e o CNPJ de quem vai receber. Não bateu, não pague.

6. QR Code falso

Como funciona: Um adesivo com outro QR Code é colado por cima do original em bares, feiras e estacionamento. O Pix vai para o golpista.

Sinal de alerta: Adesivo com borda ou brilho diferente; nome do recebedor que não é o do estabelecimento.

O que fazer: Antes de confirmar o Pix, confira o nome e o valor na tela do app.

7. Comprovante falso de Pix

Como funciona: O "comprador" mostra um print de comprovante editado e leva o produto antes de o dinheiro cair.

Sinal de alerta: Pressa para levar e insistência no print.

O que fazer: Só entregue depois de ver o dinheiro no extrato do app.

8. Pix agendado e cancelado

Como funciona: O comprador mostra o comprovante de um Pix agendado, pega o produto e cancela o agendamento antes da data.

Sinal de alerta: Comprovante com a palavra "agendado".

O que fazer: Agendamento não é pagamento. Entregue só com o dinheiro na conta.

9. Pix enviado "por engano"

Como funciona: O golpista manda um Pix para você e pede a devolução para outra chave. Depois, ainda pede o dinheiro de volta ao banco alegando fraude.

Sinal de alerta: Pedido para devolver numa chave diferente da que enviou.

O que fazer: Devolva só pelo botão "devolver" da própria transação no app. Nunca para outra conta.

10. Falso empréstimo com taxa

Como funciona: Prometem crédito fácil, até para negativado. Depois do cadastro, o empréstimo é "aprovado", mas só sai se você pagar uma taxa antes. O dinheiro nunca chega.

Sinal de alerta: Pedir dinheiro para liberar dinheiro.

O que fazer: Não pague nada antecipado. Confira se a empresa é autorizada pelo Banco Central.

11. Golpe em nome da Febraban

Como funciona: Mensagem ou perfil com a logo da Febraban fala de um "assunto urgente" ou transação suspeita e pede dados ou pagamento.

Sinal de alerta: Contato da Febraban com pessoa física.

O que fazer: A Febraban não contata clientes por SMS, ligação, e-mail, WhatsApp ou redes sociais. Ignore e bloqueie.

12. Falso "valores a receber"

Como funciona: Anúncio ou vídeo falso promete resgatar dinheiro esquecido no banco e leva a um site parecido com o gov.br, que cobra uma taxa.

Sinal de alerta: Taxa para resgatar valores, link recebido por mensagem ou app de "consulta".

O que fazer: O serviço do Banco Central é gratuito e só no site oficial. O BC não tem app para isso nem manda links.

13. Chupa-cabra no caixa eletrônico

Como funciona: Um aparelho escondido no leitor do caixa copia o cartão, e uma câmera ou teclado falso grava a senha. Às vezes alguém se oferece para "ajudar".

Sinal de alerta: Leitor solto ou torto, teclado diferente, desconhecido oferecendo ajuda, adesivo com 0800 no caixa.

O que fazer: Cubra o teclado ao digitar, recuse ajuda e, se o cartão prender, ligue para o banco pelo número do cartão.

14. Falso parente: "troquei de número"

Como funciona: Com a foto de um parente, o golpista manda mensagem de um número novo, conta uma emergência e pede um Pix.

Sinal de alerta: Número novo, pressa e pedido de dinheiro.

O que fazer: Ligue para o número antigo ou confirme por outro canal antes de qualquer Pix.

15. Clonagem do WhatsApp

Como funciona: O golpista pede o código de 6 dígitos que chegou por SMS. Com ele, assume sua conta e pede dinheiro aos seus contatos.

Sinal de alerta: Qualquer pessoa pedindo um código que chegou no seu celular.

O que fazer: Nunca passe o código. Ative a confirmação em duas etapas no WhatsApp.

16. Voz clonada por IA

Como funciona: Ligações mudas gravam um simples "alô". Com inteligência artificial, a voz é imitada num áudio para um parente, pedindo dinheiro.

Sinal de alerta: Áudio com a voz de alguém próximo pedindo Pix com urgência.

O que fazer: Ligue de volta para a pessoa. Combine uma palavra secreta com a família.

17. Amigo invadido vendendo investimento

Como funciona: A conta de um conhecido é invadida e passa a postar lucros com cripto ou investimento. Os amigos confiam e depositam.

Sinal de alerta: Conhecido que de repente divulga lucro alto e rápido.

O que fazer: Confirme com a pessoa por ligação. Recomendação de conhecido não prova nada se a conta foi invadida.

18. Falso aviso de direitos autorais

Como funciona: Mensagem diz que sua conta será desativada por violar direitos autorais e manda um link de "recurso". Em outra versão, derrubam o perfil com denúncia falsa e cobram para retirar.

Sinal de alerta: Prazo curto, link externo ou pedido de pagamento para manter a conta.

O que fazer: Não clique nem pague. Confira os avisos só dentro do app, em Configurações e na Central de Ajuda.

19. Golpe da tarefa

Como funciona: Oferecem dinheiro para curtir vídeos ou avaliar lojas. Pagam centavos no começo e depois pedem que você deposite para "liberar" ganhos maiores.

Sinal de alerta: Pagamento por curtida e pedido de depósito para continuar.

O que fazer: Ninguém paga de verdade por curtidas. Saia da conversa e não deposite.

20. Golpe do amor

Como funciona: Um perfil cria um romance pela internet e, depois de ganhar confiança, inventa uma emergência ou viagem e pede dinheiro.

Sinal de alerta: Só conhece pela internet, evita chamada de vídeo e encontro, e pede dinheiro.

O que fazer: Não envie dinheiro. Guarde as conversas e denuncie, mesmo com vergonha.

21. Sextorsão

Como funciona: Depois de uma conversa íntima, o golpista ameaça divulgar fotos ou vídeos se você não pagar. Pagar costuma trazer novos pedidos.

Sinal de alerta: Ameaça de expor conteúdo íntimo em troca de dinheiro.

O que fazer: Não pague. Guarde as provas, procure a polícia e o canal de ajuda da SaferNet.

22. Loja falsa nas redes

Como funciona: Um perfil novo anuncia produtos muito abaixo do preço, com pressa ("só hoje"), e pede Pix. O produto nunca chega.

Sinal de alerta: Preço bom demais, perfil recente, comentários fechados, sem CNPJ, Pix para pessoa física.

O que fazer: Pesquise a loja antes. Se pagou, peça o MED ao banco e registre reclamação no Procon e boletim de ocorrência.

23. Vídeo falso de autoridade ou famoso

Como funciona: Um vídeo feito com inteligência artificial mostra uma autoridade ou celebridade anunciando benefício, investimento ou produto, com link para um site falso.

Sinal de alerta: Famoso prometendo dinheiro fácil num anúncio, com link fora do site oficial.

O que fazer: Procure a notícia em sites oficiais. Benefício do governo só em gov.br.

24. Falso Procon

Como funciona: Mensagem em nome do Procon fala de uma reclamação ou indenização e pede um Pix para dar andamento.

Sinal de alerta: Órgão de defesa do consumidor pedindo depósito.

O que fazer: O Procon não pede Pix nem depósito. Confirme pelo site oficial do Procon do seu estado.

25. Dinheiro fácil viral

Como funciona: Posts e vídeos que viralizam prometem renda extra, bônus ou ganho rápido, quase sempre com pagamento só por Pix.

Sinal de alerta: Promessa de vantagem financeira com pagamento antecipado por Pix.

O que fazer: Desconfie de ganho fácil. Se pede dinheiro antes, é golpe.

26. Falso comprador com link de pagamento

Como funciona: Você anuncia algo e o "comprador" manda um link para você "receber o pagamento". A página falsa pede seus dados, senha ou uma taxa de desbloqueio.

Sinal de alerta: Link de pagamento enviado pelo comprador, dentro ou fora do app.

O que fazer: Plataformas não mandam links no chat. Mantenha a venda no fluxo oficial e confira o dinheiro no seu banco.

27. Falso intermediário na venda de carro

Como funciona: O golpista copia o anúncio de um carro real, anuncia mais barato e fica no meio da negociação. Pede que comprador e vendedor não falem de preço. O comprador paga a ele e os dois ficam no prejuízo.

Sinal de alerta: Pedido para não conversar sobre o valor com a outra parte; preço bem abaixo da tabela.

O que fazer: Converse direto com o dono e pague só na transferência no Detran, para a conta do proprietário.

28. Aluguel de temporada falso

Como funciona: Fotos de um imóvel real viram um anúncio falso de temporada. Pedem um sinal por Pix para reservar, e o imóvel nunca é entregue.

Sinal de alerta: Preço abaixo do normal, pressa pelo sinal, Pix fora da plataforma, perfil novo e sem avaliações.

O que fazer: Reserve por plataformas que intermediam o pagamento e confira se o nome do Pix é o do anunciante.

29. Ingresso falso

Como funciona: Em show disputado ou esgotado, aparecem sites quase iguais aos oficiais e revendedores nas redes vendendo ingressos que não existem.

Sinal de alerta: Show esgotado com ingresso sobrando, preço abaixo do oficial, venda por mensagem e pagamento por Pix.

O que fazer: Compre só no site oficial ou na bilheteria. Na revenda, use plataforma que transfere o ingresso para o seu nome.

30. Site clone de loja famosa

Como funciona: Criminosos copiam o visual de uma grande loja, registram um endereço parecido e anunciam preços muito baixos. O pagamento vai para um CPF qualquer.

Sinal de alerta: Endereço do site com letras trocadas ou palavras a mais; Pix para pessoa física.

O que fazer: Digite o endereço da loja você mesmo ou use o app oficial. Confira o nome de quem recebe o Pix.

31. Anúncio patrocinado falso

Como funciona: O golpista paga para aparecer no topo da busca com um anúncio que leva a um site falso de loja, ingresso ou serviço.

Sinal de alerta: Primeiro resultado com o selo "patrocinado" levando a um endereço diferente do oficial.

O que fazer: Prefira o resultado com o endereço oficial e denuncie o anúncio falso.

32. Taxa para liberar encomenda

Como funciona: SMS ou mensagem diz que sua encomenda está retida e pede uma taxa por link. O site imita o dos Correios ou de uma transportadora.

Sinal de alerta: Cobrança por link para liberar entrega; endereço que não é o oficial.

O que fazer: Confira o rastreio só no site oficial, digitando o endereço. Não pague por link de mensagem.

33. Maquininha com visor quebrado

Como funciona: Um falso entregador cobra uma taxa pequena na maquininha com o visor danificado. Em vez de R\$ 4,90, digita R\$ 4.900.

Sinal de alerta: Taxa inesperada na entrega e visor que não deixa ver o valor.

O que fazer: Pague pelo app de delivery, que não cobra extra na entrega. Confira o valor antes de digitar a senha.

34. Falso presente

Como funciona: Alguém liga avisando que há um presente ou brinde para você. Na entrega, cobram uma "taxa simbólica" na maquininha, que registra um valor muito maior.

Sinal de alerta: Presente que você não esperava e taxa para receber.

O que fazer: Recuse entrega com taxa que você não combinou. Na dúvida, pergunte a quem teria mandado.

35. Leilão falso de veículos

Como funciona: Sites que imitam Detran ou leiloeiros mostram carros pela metade do preço. Depois do "arremate", mandam um termo falso e uma chave Pix. O carro não existe.

Sinal de alerta: Preço muito abaixo do mercado, site com endereço diferente do oficial, pagamento por Pix.

O que fazer: Confira leilões só no site oficial do Detran do seu estado e nunca pague sem ver o veículo.

36. Sorteio falso de marca

Como funciona: Um perfil que imita uma loja ou influenciador anuncia um sorteio e diz que você ganhou. Para receber, pede seus dados ou o pagamento do frete.

Sinal de alerta: Prêmio que pede pagamento de frete ou taxa; perfil com nome parecido com o da marca.

O que fazer: Confira o sorteio no perfil verificado e no site oficial. Sorteio de verdade não cobra para entregar.

37. Consórcio contemplado falso

Como funciona: Anunciam uma carta de consórcio "já contemplada" com parcelas baixas. Você paga uma taxa de transferência e o vendedor some.

Sinal de alerta: Carta contemplada oferecida por mensagem ou ligação, com taxa antes de qualquer documento.

O que fazer: Confirme com a administradora e veja se ela é autorizada pelo Banco Central.

99. Aluguel de imóvel falso

Como funciona: Um falso proprietário ou corretor anuncia um imóvel bem localizado e barato e pede caução ou o primeiro aluguel antes da visita. Depois some.

Sinal de alerta: Pagamento antes de visitar e assinar contrato; corretor sem Creci.

O que fazer: Não pague antes da visita e do contrato. Confira o Creci do corretor.

38. Falsa vaga de emprego com taxa

Como funciona: Um "recrutador" oferece uma vaga com bom salário em empresa conhecida e cobra taxa de inscrição, exame, curso ou uniforme. Depois some.

Sinal de alerta: Qualquer cobrança para participar de seleção ou ser contratado.

O que fazer: Empresa séria não cobra para contratar. Confirme a vaga no site oficial da empresa.

39. Recrutador falso com teste infectado

Como funciona: Um falso recrutador, muitas vezes no LinkedIn, manda um "teste técnico", um arquivo ou um link de videochamada que instala um programa espião.

Sinal de alerta: Processo seletivo que pede para baixar e rodar arquivos ou instalar programas.

O que fazer: Confirme o recrutador no site da empresa e não rode arquivos de desconhecidos no seu computador.

40. Kit de trabalho em casa

Como funciona: Depois de uma "contratação" rápida, pedem que você pague o envio de equipamentos, documentos ou um kit inicial para começar.

Sinal de alerta: Ter que pagar para começar a trabalhar.

O que fazer: Não pague. Empresa que contrata de verdade arca com o próprio material.

41. Pirâmide financeira

Como funciona: Prometem ganho alto e rápido, e o lucro vem de quem entra depois, não de um negócio real. Quando as entradas param, tudo desmorona.

Sinal de alerta: Lucro garantido, bônus por indicar pessoas, empresa sem autorização da CVM.

O que fazer: Desconfie de rendimento muito acima do mercado e consulte a empresa no site da CVM.

42. Falso assessor de investimentos

Como funciona: Alguém se apresenta como assessor de uma corretora conhecida, oferece uma oportunidade "exclusiva" e pede transferência para uma conta que não é da corretora.

Sinal de alerta: Contato que você não pediu, retorno alto e pedido de Pix para pessoa física.

O que fazer: Assessor de verdade não pede depósito em conta pessoal. Confirme pelos canais oficiais da corretora.

43. Grupo de investimento com prints de lucro

Como funciona: Você é colocado num grupo de WhatsApp ou Telegram cheio de prints de ganhos. Para entrar na "operação" ou sacar o lucro, pedem depósitos.

Sinal de alerta: Prints de lucro de outros membros e pedido de depósito para liberar saque.

O que fazer: Saia do grupo. Ganho garantido não existe, e saque que exige depósito é golpe.

44. Corretora sem autorização

Como funciona: Plataformas de fora do país oferecem investimentos ou negociação para brasileiros sem autorização da CVM.

Sinal de alerta: Empresa estrangeira que não aparece na lista da CVM.

O que fazer: Antes de investir, consulte no site da CVM se a empresa é autorizada.

45. App que paga para ver vídeos

Como funciona: Um aplicativo promete dinheiro para assistir vídeos ou anúncios. O saldo sobe rápido, mas o saque nunca sai ou exige uma taxa.

Sinal de alerta: Saldo que cresce rápido demais e cobrança para liberar o saque.

O que fazer: App que pede depósito para pagar você é golpe. Pesquise a reputação antes de instalar.

46. Falso recuperador de dinheiro

Como funciona: Quem já caiu em golpe é procurado por alguém que promete recuperar o dinheiro, às vezes fingindo ser polícia ou órgão público, mediante uma taxa.

Sinal de alerta: Promessa de recuperar valores com pagamento antecipado.

O que fazer: É o segundo golpe. Procure só o seu banco e a polícia, e não pague taxas.

47. Jogo de apostas com influenciador

Como funciona: Influenciadores pagos mostram ganhos falsos em jogos como o "tigrinho". As plataformas são clandestinas, e o prêmio só "sai" se você pagar uma taxa. Depois, a conta é bloqueada.

Sinal de alerta: Influenciador ostentando ganhos fáceis e cobrança para liberar prêmio.

O que fazer: Não deposite em plataformas divulgadas assim. Se pagou, registre boletim de ocorrência.

48. CNH suspensa ou multa por SMS

Como funciona: Um SMS diz que sua CNH será suspensa ou que há uma multa com desconto, e manda um link para um site parecido com o gov.br que cobra uma "taxa".

Sinal de alerta: Detran mandando link por SMS, e-mail ou WhatsApp.

O que fazer: Os Detrans não avisam suspensão nem cobram multa por mensagem. Consulte no site oficial ou na Carteira Digital de Trânsito.

49. Falso servidor do INSS

Como funciona: Alguém liga, manda SMS ou até aparece em casa com crachá dizendo que a prova de vida está pendente e que o benefício será bloqueado. Pede dados, senha ou dinheiro.

Sinal de alerta: Aviso de prova de vida pendente por mensagem ou visita.

O que fazer: O INSS faz a prova de vida automaticamente e não visita para isso. Confirme no app Meu INSS ou na Central 135.

50. Falso advogado

Como funciona: Com dados reais do seu processo, alguém se passa pelo seu advogado e diz que há dinheiro a receber. Para liberar, pede uma "taxa" por Pix.

Sinal de alerta: Número novo do "advogado", urgência e taxa para liberar valores.

O que fazer: A Justiça não cobra para liberar indenização. Ligue para o seu advogado no número que você já tinha.

51. Precatório com taxa

Como funciona: Quem tem precatório a receber é procurado por um falso escritório que diz que o pagamento depende de depósito de custas ou certidões.

Sinal de alerta: Cobrança para liberar precatório por telefone, mensagem ou e-mail.

O que fazer: A Justiça não exige depósito para liberar precatório. Consulte o processo no site do tribunal.

52. Falso oficial de justiça

Como funciona: Uma mensagem fala de intimação, audiência ou processo e manda um link para "ver o mandado". O link rouba dados ou pede pagamento.

Sinal de alerta: Link para visualizar mandado, pedido de dados ou de dinheiro.

O que fazer: Tribunal não pede senha nem dinheiro. Confirme a intimação pelos canais oficiais do fórum.

53. Restituição falsa do Imposto de Renda

Como funciona: E-mail ou SMS diz que sua restituição está liberada ou retida e manda um link para um site que imita a Receita, pedindo dados ou uma taxa.

Sinal de alerta: Mensagem da "Receita" com link.

O que fazer: Os avisos da Receita não têm link. Consulte a restituição no e-CAC, com a sua conta gov.br.

54. Cobrança falsa da Receita com seus dados

Como funciona: Uma página igual ao gov.br aparece com seu nome e CPF verdadeiros e cobra um "débito" para pagamento imediato.

Sinal de alerta: Dívida desconhecida cobrada por link, com prazo curto.

O que fazer: Pendências com a Receita só aparecem no e-CAC. A Receita não cobra por link.

55. Falso programa social

Como funciona: Mensagens anunciam inscrições abertas para CNH Social, Bolsa Família ou outro benefício, com link para cadastro. O site coleta seus dados ou cobra uma guia.

Sinal de alerta: Inscrição por link de mensagem, taxa para liberar benefício, pedido para compartilhar com amigos.

O que fazer: Confira sempre no site oficial do órgão, com final gov.br. Benefício não cobra taxa.

56. Falso Desenrola

Como funciona: Anúncios e sites falsos usam o nome do Desenrola Brasil, prometem descontos enormes nas dívidas e pedem CPF, dados bancários ou uma "taxa administrativa".

Sinal de alerta: Desconto exagerado, intermediário e cobrança antecipada.

O que fazer: O Desenrola não tem intermediários nem cobra antes. Acesse só pelo site oficial gov.br.

57. Falso "limpa nome"

Como funciona: Perfis e mensagens em nome da Serasa oferecem quitar dívidas com descontos de até 99% por um boleto ou Pix. O nome continua sujo e o dinheiro some.

Sinal de alerta: Contato pelas redes oferecendo acordo, desconto exagerado e prazo curto.

O que fazer: Negocie só pela plataforma oficial e use o validador de boletos dela antes de pagar.

58. Conta de luz falsa

Como funciona: Mensagem com a logo da distribuidora fala de conta atrasada, ameaça corte e manda um boleto ou link. O beneficiário é o golpista.

Sinal de alerta: Ameaça de corte por mensagem de número sem verificação; beneficiário estranho no boleto.

O que fazer: Emita a fatura no app ou site oficial da distribuidora e confira o beneficiário antes de pagar.

92. Falso programa de nota fiscal

Como funciona: Mensagens em nome de programas estaduais de nota fiscal premiada pedem para "validar o acesso" ou resgatar prêmio por link.

Sinal de alerta: Link por WhatsApp para validar cadastro ou receber prêmio.

O que fazer: Os programas não mandam links por WhatsApp. Acesse pelo site oficial da Secretaria da Fazenda.

96. Ameaça de bloqueio do CPF

Como funciona: E-mail ou página que imita a Receita diz que seu CPF será suspenso por uma multa e oferece um "auditor" no chat para pagar por Pix com cronômetro.

Sinal de alerta: Ameaça ao CPF, prazo curto, pagamento por Pix.

O que fazer: Confira sua situação no site oficial da Receita, que termina em gov.br.

97. Falsa multa de órgão federal

Como funciona: E-mails, SMS ou ligações usam o nome da PRF ou de outros órgãos para cobrar multas falsas com link para pagamento.

Sinal de alerta: Multa por mensagem com link e prazo curto.

O que fazer: Consulte multas só nos sites oficiais. Órgão federal termina em gov.br.

59. Troca de chip (SIM swap)

Como funciona: O golpista se passa por você na operadora e transfere seu número para outro chip. Seu celular perde o sinal e ele passa a receber seus códigos por SMS.

Sinal de alerta: Celular sem sinal de repente, sem motivo.

O que fazer: Ligue já para a operadora por outro aparelho. Ative o PIN do chip e prefira app autenticador a SMS.

60. Número falso na tela

Como funciona: O golpista mascara o número da chamada para aparecer como o do banco (como 4004 ou 3004). A ligação parece oficial, mas não é.

Sinal de alerta: Ligação "do banco" pedindo dados ou transferência, mesmo com número conhecido.

O que fazer: Desligue e ligue você mesmo para o número do cartão ou do app.

61. SMS de antena falsa

Como funciona: Criminosos usam uma antena clandestina para mandar SMS que parecem da operadora ou do banco, com links de compra não reconhecida, prêmio ou bloqueio.

Sinal de alerta: SMS "oficial" com link e urgência.

O que fazer: Não clique. Confira no app oficial do banco ou da operadora.

62. QR Code do WhatsApp Web

Como funciona: Com uma desculpa qualquer, pedem que você escaneie um QR Code com o WhatsApp. Ele conecta a sua conta ao computador do golpista, que lê suas conversas.

Sinal de alerta: Alguém pedindo para você escanear um QR Code com o WhatsApp.

O que fazer: Só escaneie QR Code em web.whatsapp.com aberto por você. Revise os aparelhos conectados no app.

63. WhatsApp modificado

Como funciona: Versões piratas como o "WhatsApp GB" prometem funções extras, mas vêm de fontes desconhecidas, pedem acesso a todos os arquivos e podem trazer programas espiões.

Sinal de alerta: Download do WhatsApp fora da loja oficial.

O que fazer: Use só o app oficial. Além do risco, o WhatsApp pode banir a conta.

64. App falso de banco

Como funciona: Um aplicativo que imita banco ou carteira digital pede a permissão de acessibilidade. Com ela, o programa controla a tela e pode fazer Pix sem você ver.

Sinal de alerta: App pedindo permissão de acessibilidade ou instalação fora da loja.

O que fazer: Instale só pela loja oficial e negue acessibilidade a apps que não precisam dela.

65. Falso suporte técnico

Como funciona: Uma tela de alerta com sirene diz que o computador está infectado e mostra um número para ligar. Quem atende pede acesso remoto e pagamento.

Sinal de alerta: Aviso de vírus no navegador com telefone para ligar.

O que fazer: A Microsoft não manda alerta de vírus com telefone. Feche o navegador e não ligue.

66. "Seu iPhone foi encontrado"

Como funciona: Depois de um roubo, chega uma mensagem dizendo que o aparelho foi localizado, com link para um login falso do iCloud. A senha serve para desbloquear o celular roubado.

Sinal de alerta: Mensagem sobre o aparelho perdido pedindo login.

O que fazer: Não clique. Use só o app ou site oficial de Buscar e troque a senha pelo site oficial.

67. Falso aviso de streaming

Como funciona: E-mail ou SMS com a cara da Netflix ou de outro streaming diz que o pagamento falhou e pede para "atualizar o cartão" num link.

Sinal de alerta: Ameaça de suspensão com prazo e link para pagamento.

O que fazer: Confira a assinatura pelo app oficial. Se digitou o cartão, avise o banco.

68. Login falso por e-mail

Como funciona: E-mails dizem que sua senha expirou, que há um alerta de segurança ou que é preciso confirmar um aparelho, e levam a uma página de login falsa.

Sinal de alerta: E-mail pedindo login para "não perder o acesso".

O que fazer: Entre na conta digitando o endereço oficial. Nunca pelo botão do e-mail.

69. Wi-Fi público falso

Como funciona: Em aeroportos e locais cheios, alguém cria uma rede com nome parecido com a oficial. Quem se conecta cai numa página falsa que rouba dados.

Sinal de alerta: Duas redes com nomes quase iguais, ou rede pedindo muitos dados para conectar.

O que fazer: Confirme o nome da rede com o local e use os dados móveis para acessar o banco.

100. Telefone falso no buscador

Como funciona: Ao procurar o atendimento de uma empresa na internet, você encontra um número falso em anúncio ou site. Quem atende se passa pela empresa e pede dados, acesso ou pagamento.

Sinal de alerta: Número de atendimento achado em anúncio ou site que não é o oficial.

O que fazer: Pegue o telefone no app, na fatura ou no site oficial da empresa.

70. Bilhete premiado

Como funciona: Na rua, alguém diz ter um bilhete de loteria premiado que não pode resgatar. Um comparsa "desconhecido" ajuda a convencer, e a vítima entrega dinheiro ou saca no banco para "comprar" o prêmio.

Sinal de alerta: Desconhecido com um prêmio que não pode receber e quer dividir com você.

O que fazer: Não negocie nada com estranhos na rua. Em flagrante, ligue 190.

71. Troca de cartão na maquininha

Como funciona: O vendedor diz que a senha não passou, pede para tentar em outra máquina e, na distração, devolve um cartão parecido. A primeira máquina já gravou sua senha.

Sinal de alerta: Falha estranha na maquininha, troca de aparelho, visor danificado.

O que fazer: Insira e retire o cartão você mesmo e confira se o cartão devolvido é o seu.

72. Falso técnico da operadora

Como funciona: Alguém com uniforme de operadora aparece sem aviso para "manutenção" ou "troca de modem" e aproveita para furtar ou pedir dados e pagamentos.

Sinal de alerta: Visita sem agendamento e sem número de protocolo.

O que fazer: Confirme a visita no app ou no telefone oficial da operadora antes de abrir a porta.

73. Falso motorista no aeroporto

Como funciona: No desembarque, alguém se oferece como motorista de aplicativo, leva o passageiro e cobra muitas vezes o valor normal, às vezes com ameaças.

Sinal de alerta: Abordagem no saguão oferecendo corrida fora do app.

O que fazer: Peça a corrida só pelo app ou use serviço credenciado do aeroporto. Confira o carro e a placa.

74. Código de entrega no delivery

Como funciona: Um falso entregador diz que não acha o endereço e pede seu número por WhatsApp. Com os últimos dígitos, confirma a entrega sem entregar nada.

Sinal de alerta: Entregador pedindo seu número ou o código antes de chegar.

O que fazer: Passe o código só com o pedido na mão, na sua porta. Use o chat do app.

75. Aproximação na multidão

Como funciona: Em aglomerações, criminosos se passam por ambulantes ou encostam maquininhas para cobrar por aproximação. A Febraban orienta cuidado, embora as empresas de cartão digam não ter registros concretos.

Sinal de alerta: Cobrança por aproximação sem você pedir, em lugar lotado.

O que fazer: Em festas e blocos, desative a aproximação ou use o cartão só pela carteira do celular.

76. Falso sequestro

Como funciona: Uma ligação com alguém gritando diz que um parente foi sequestrado e exige Pix na hora. Muitas dessas ligações saem de presídios.

Sinal de alerta: Ligação desesperada exigindo pagamento imediato e sem deixar desligar.

O que fazer: Desligue e ligue para o parente. Em dúvida, chame a polícia pelo 190.

77. Falso policial

Como funciona: Alguém se apresenta como policial federal, diz que você é investigado e manda transferir dinheiro para uma "conta de vigilância". Às vezes simula audiência por vídeo.

Sinal de alerta: Polícia cobrando dinheiro por telefone ou mensagem.

O que fazer: A polícia não cobra valores por telefone. Desligue e procure uma delegacia.

78. Agência investigada e "conta segura"

Como funciona: Dizem que seu gerente ou sua agência está sendo investigada e que é preciso mover o dinheiro para uma "conta segura", às vezes com boletim de ocorrência falso.

Sinal de alerta: Pedido para transferir tudo para outra conta "para proteger".

O que fazer: Conta segura não existe. Banco nunca pede transferência para outra conta.

79. Falso gerente

Como funciona: Com a foto e o nome de um gerente real, o golpista fala por WhatsApp ou liga, pede para "validar" uma transação por link ou para movimentar dinheiro.

Sinal de alerta: Gerente falando de número pessoal, com urgência e link.

O que fazer: Desligue e fale com o banco pelo app ou pelo número oficial.

80. Falso médico do hospital

Como funciona: Com dados reais de um paciente internado, alguém liga para a família dizendo ser médico e pede Pix urgente para um exame ou remédio "particular".

Sinal de alerta: Pedido de Pix para pessoa física em nome do hospital.

O que fazer: Hospital não cobra por telefone. Confirme com a equipe pelo número oficial.

81. Videochamada falsa com IA

Como funciona: Com fotos e vídeos das redes, a inteligência artificial imita rosto e voz de um parente numa videochamada que pede dinheiro para uma emergência.

Sinal de alerta: Emergência com pedido de transferência imediata, mesmo vendo o rosto da pessoa.

O que fazer: Desligue e ligue para o número salvo. Combine uma palavra secreta com a família.

82. Golpes no luto

Como funciona: Golpistas criam vaquinhas falsas em nome de famílias de vítimas de tragédias, ou se passam por cemitério e funerária para cobrar planos e serviços por mensagem.

Sinal de alerta: Pedido de doação ou pagamento por canal não oficial em momento de luto.

O que fazer: Doe só pelo canal divulgado pela família. Pague funerária e cemitério só com documento oficial.

83. Remédio milagroso

Como funciona: Vídeos com famosos ou "médicos" criados por IA vendem remédios e suplementos milagrosos, quase sempre clandestinos ou falsificados.

Sinal de alerta: Cura rápida prometida em anúncio, com celebridade ou médico sem CRM.

O que fazer: Consulte a Anvisa sobre o produto e compre remédio só em farmácia regularizada.

84. Plano de saúde falso

Como funciona: Uma falsa corretora oferece plano barato, sem carência, e cobra por boleto ou Pix. O plano nunca existiu. Em outra versão, chega um boleto falso da sua operadora.

Sinal de alerta: Preço muito abaixo do mercado, sem carência, pagamento para pessoa física.

O que fazer: Confira a operadora no site da ANS e o beneficiário de qualquer boleto antes de pagar.

85. Falsa agência de viagens

Como funciona: Uma agência vende pacotes baratos, muitas vezes por Pix, e depois cancela as passagens e some sem reembolsar.

Sinal de alerta: Preço muito abaixo do normal, empresa sem cadastro no Ministério do Turismo.

O que fazer: Confira o CNPJ e o cadastro da agência no Cadastur antes de pagar.

86. Venda de milhas falsa

Como funciona: Em classificados e redes, pessoas vendem passagens com milhas por preços muito baixos. Você paga e a passagem não existe ou é cancelada.

Sinal de alerta: Desconto acima de 50% e vendedor pessoa física sem CNPJ.

O que fazer: Compre passagens direto na companhia ou em empresa com CNPJ e reputação conhecida.

87. Mensagem falsa da reserva

Como funciona: Pelo chat da plataforma de hospedagem, chega uma mensagem do "hotel" dizendo que o pagamento falhou e pedindo para confirmar o cartão num link.

Sinal de alerta: Pedido de dados do cartão por link, com ameaça de cancelar a reserva.

O que fazer: A plataforma não pede cartão fora do app. Confirme a reserva pelo app ou com o hotel.

88. Pontos expirando

Como funciona: SMS ou e-mail avisa que seus pontos ou milhas vão vencer e manda um link para resgatar. A página falsa pede dados do banco e senhas.

Sinal de alerta: Pontuação alta e redonda que você não lembra, com link para resgate.

O que fazer: Confira os pontos só no app oficial do programa.

89. Doação falsa em tragédia

Como funciona: Depois de enchentes e desastres, golpistas espalham chaves Pix e vaquinhas falsas em posts, comentários e mensagens.

Sinal de alerta: Chave Pix em comentário ou mensagem, sem confirmação do órgão ou da entidade.

O que fazer: Doe só pela chave divulgada no canal oficial e confira o nome de quem recebe.

90. Bolão falso

Como funciona: Sites e anúncios imitam a Caixa e vendem bolões da Mega da Virada que não geram aposta nenhuma. Também há bolões informais vendidos na rua.

Sinal de alerta: Site que não é o oficial da Caixa e venda de bolão fora da lotérica.

O que fazer: Aposte só em lotéricas, no app ou no site oficial Loterias Caixa.

91. Promoção que pede para compartilhar

Como funciona: Uma "pesquisa de satisfação" ou promoção de marca conhecida promete prêmio (passagem, plano, dinheiro) e pede que você repasse para dezenas de contatos. No fim, rouba dados ou instala programas.

Sinal de alerta: Prêmio grátis que exige repassar a mensagem.

O que fazer: Não repasse. Confira a promoção no site oficial da marca.

93. "Eu gravei você"

Como funciona: Um e-mail diz que hackers gravaram você pela webcam e exige pagamento em cripto. Para assustar, mostra uma senha sua de um vazamento antigo. Não existe gravação.

Sinal de alerta: Ameaça genérica com prazo, pedido em bitcoin, senha antiga sua.

O que fazer: Não pague nem responda. Troque a senha mostrada e ative a verificação em duas etapas.

94. Romance com investimento

Como funciona: Alguém conhecido em app de namoro ou por "mensagem errada" puxa conversa por semanas e depois apresenta uma plataforma de cripto onde "ganha muito". Você investe e não consegue sacar.

Sinal de alerta: Contato que vira amizade ou romance e chega a investimentos.

O que fazer: Não invista por indicação de quem você só conhece online.

95. Falso suporte de carteira cripto

Como funciona: Um falso suporte, e-mail, carta ou site pede sua frase de recuperação para "validar" a carteira. Com ela, o golpista leva tudo.

Sinal de alerta: Qualquer pessoa ou site pedindo a frase de recuperação.

O que fazer: Nenhum suporte legítimo pede essa frase. Guarde-a fora da internet.

98. Aluguel de conta bancária

Como funciona: Oferecem dinheiro fácil para você "emprestar" sua conta ou chave Pix. Ela passa a receber dinheiro de golpes, e quem cede a conta responde por crime.

Sinal de alerta: Proposta de pagamento para usar sua conta.

O que fazer: Nunca empreste conta ou chave Pix. Ceder a conta para golpes é crime.

Fontes

Alertas de órgãos públicos, polícias, Febraban, Procons e imprensa.
Conteúdo educativo: em caso de golpe, procure o seu banco e as autoridades.

1. Febraban: os golpes mais aplicados (Movimento Econômico, 2025)
2. Febraban alerta para golpes (O Povo, 2024)
3. Febraban: como evitar golpes bancários (Diário de Pernambuco)
4. Febraban dá dicas sobre golpe do acesso remoto
4. Golpe da mão fantasma (Serasa)
5. Golpe do boleto adulterado (Correio Braziliense)
6. Febraban emite alerta sobre QR Code falso (Mix Vale, 26/10/2026)
6. Pix e QR Code: os golpes invisíveis (Canaltech)
7. Golpes mais aplicados no Brasil em 2026 (Estado de Minas, ago/2026)
8. Golpes mais aplicados no Brasil em 2026 (Estado de Minas, ago/2026)
9. Entenda o golpe do Pix errado (O Povo, 2024)
9. Golpe do Pix errado (Canaltech)
10. Febraban alerta que criminosos usam o nome da entidade (Correio Braziliense, out/2026)
11. Febraban alerta que criminosos usam o nome da entidade (Mercado & Consumo, 09/10/2026)
12. Banco Central alerta sobre golpe dos valores a receber (JC Concursos)
12. Vídeo falso e site falso do gov.br é golpe (Agência Gov)
13. Golpe do chupa-cabra no Espírito Santo (Tribuna Online)
14. Como evitar cair em golpes bancários (Fenacon)
15. Golpes mais aplicados no Brasil em 2026 (Estado de Minas, ago/2026)
16. Polícia de SP alerta sobre o golpe da ligação muda (TNH1)
16. Polícia alerta para golpe que usa IA para clonar voz (BandNews FM)
17. Grupo que invadia contas no Instagram é alvo do MPGO (Jornal Opção)
18. Golpistas de direitos autorais no Instagram (Malwarebytes, set/2026)
18. Criadores perdem perfil em golpe de copyright (Canaltech)
19. Polícia investiga golpe da renda extra (TNH1)
20. Polícia Civil alerta para o golpe do amor (Bem Paraná, 2026)
20. Golpe do amor e as fraudes do Dia dos Namorados (TNH1, cita ABBC)
21. O que é sextorsão (Canaltech)
22. Como detectar lojas falsas no Instagram (ESET)
22. Procon orienta sobre compras seguras (Viva)
23. Golpe com deepfake de ministro leva a site falso do gov.br (Canaltech)
24. Golpistas usam o nome do Procon para exigir Pix (Tribuna PR)
25. Golpes online virais aumentam e Pix é a principal presa (Finsiders,

jun/2026)

26. Como evitar golpes na OLX (Tecnoblog)
26. OLX: como evitar golpes (Canaltech)
27. Golpista engana vendedor e comprador de carro (Metrópoles)
27. Golpe usa WhatsApp para enganar vendedores de carros (Vrum, jul/2026)
28. PCPR alerta para golpe do aluguel na temporada
28. Procon Alagoas alerta para golpes em aluguéis por temporada (TNH1)
29. Golpe do ingresso falso aumenta com grandes shows (SBT News)
29. Golpe do ingresso falso: dicas (CNN Brasil)
30. Golpes usam serviços legítimos para clonar gigantes do e-commerce (Canaltech)
31. Criminosos usam anúncios no Google para vender ingresso falso (Aos Fatos)
31. Google removeu bilhões de anúncios de golpes (Olhar Digital)
32. Correios alertam para golpe da taxa via SMS (Gazeta SP)
33. Polícia Civil do PR alerta sobre golpe do delivery e maquininhas
34. Operação prende 28 suspeitos do golpe do falso presente (SBT News)
34. Como funciona o golpe do entregador de presente falso (Jovem Pan)
35. Detran-PR alerta sobre falsos leilões de veículos
35. Golpe do falso leilão imita Detran e Receita (Gazeta SP)
36. Golpe usa promoção falsa da Farm (Aos Fatos)
36. Golpe no WhatsApp promete sorteios falsos (Canaltech)
37. O golpe da falsa carta de crédito contemplada (Migalhas)
37. Como funciona um golpe de consórcio (Olhar Digital)
38. Febraban alerta: criminosos usam vagas falsas (meutudo, mai/2026)
38. Golpe do falso emprego se espalha na internet (Band, 2026)
39. Golpe da vaga mira devs e instala malware em videochamada falsa (TecMundo)
39. Vagas no LinkedIn usadas como isca para malware (Canaltech)
40. Golpes comuns no LinkedIn: ofertas falsas de emprego (ESET)
41. CVM vê indícios de pirâmide na Original Energy (Suno)
41. Pirâmide financeira: o que é e como fugir (BB Investalk)
42. Golpes no Telegram (Serasa)
43. WhatsApp vai alertar sobre golpes em grupos criados por desconhecidos (TecMundo)
44. CVM alerta sobre empresas de fora do país (Suno)
45. Renda com vídeos é golpe? (Serasa)
46. Recovery scams: falsos serviços de recuperação de dinheiro (ESET)
46. Caiu em golpe com cripto? Cuidado para não ser vítima duas vezes (Canaltech)

47. Polícia Civil registra mais de 500 BOs contra o jogo do tigrinho (Gazeta SP)
47. Como golpistas usam influenciadores para promover o jogo do tigrinho (Jornal Opção)
48. 5 dicas para evitar o golpe da multa falsa do Detran (Olhar Digital)
48. Detran-RJ alerta para golpes em nome do órgão (Tribuna do Sertão)
49. INSS alerta beneficiários sobre golpe da prova de vida (Estado de Minas)
50. Febraban alerta sobre o golpe do falso advogado (Jornal de Brasília)
50. Nubank emite alerta sobre golpe do falso advogado (Tecnoblog)
51. TRF3 alerta sobre golpe em pagamento de precatórios
52. TJMT: falsos oficiais de justiça usam WhatsApp para aplicar golpes (2026)
52. TRT-SC: golpistas se passam por oficiais de justiça
53. Receita Federal alerta para golpe na restituição (Fenacon)
53. Número de golpes dobra na época do IR (Money Times)
54. Falsas cobranças da Receita usam dados reais (Mais Goiás, jul/2026)
54. Golpistas usam CPF real para criar cobranças falsas (Estado de Minas)
55. Fake news da CNH Social: como identificar sites falsos (Portal do Trânsito)
55. Beneficiários do Bolsa Família são alvo de golpe do link falso (Band)
56. Governo alerta para tentativas de golpe no Desenrola Brasil (Convergência Digital)
56. Golpes usam Desenrola com link falso nas redes (meutudo, ago/2026)
57. Feirão sem fraude: Serasa dá dicas para evitar golpes
58. Golpe da conta de luz usa dados de clientes em Goiás (Jornal Opção)
58. Cemig lança ferramenta para confirmar a conta de luz (Agência Minas)
59. SIM swap: entenda como funciona o golpe (O Povo, 2024)
60. Após alerta do Itaú, Anatel decide bloquear operadoras que facilitam spoofing (Tecnoblog)
61. Golpe da antenna falsa: como se proteger (Serasa)
62. QRLjacking: o roubo de WhatsApp via QR Code (Tecnoblog)
62. Golpe sequestra WhatsApp com ajuda da vítima (Olhar Digital)
63. O WhatsApp GB e os riscos de apps não validados (ESET)
63. O WhatsApp pirata que abre as portas do celular (Correio Braziliense)
64. Falsos apps para Android exploram empresas brasileiras para roubos via Pix (Canaltech)
65. Golpe do suporte técnico: como identificar alertas falsos (Lock.pub)
66. Criminosos usam falsos e-mails para desbloquear iPhones roubados (Oficina da Net)
67. Site falso da Netflix tenta roubar cartões de brasileiros (Olhar Digital)
67. E-mail falso usa a Netflix para roubar dados (TecMundo)
68. Novo golpe no Brasil rouba contas Microsoft sem usar senha (Canaltech)
68. Novo golpe emite alerta falso do Google (Correio Braziliense)

69. Homem cria Wi-Fi falso para roubar dados em aviões e é preso (TecMundo)
69. Como evitar golpes em aeroportos (Canaltech)
70. Golpe do bilhete premiado: como se proteger (Viva)
70. Idosa entrega R\$ 20 mil após cair no golpe do bilhete premiado (Tribuna PR)
71. Golpe da troca de cartão: 5 dicas (Estado de Minas, out/2025)
71. Golpe do cartão trocado se espalha pelo Brasil (Canaltech)
72. E-book de conscientização contra golpes (Claro)
73. Chefe de quadrilha de falsos motoristas é preso em Guarulhos (Band, jun/2026)
74. iFood: cliente denuncia golpe da confirmação de entrega (Canaltech)
75. Dicas para pagamentos em maquininhas no Carnaval (Correio da Manhã, cita Febraban)
75. Golpes com cartões no Carnaval (ABCdoABC, cita Febraban e Abecs)
76. Golpe do Pix e falso sequestro mobilizam polícia em Vitória (A Gazeta)
77. Criminosos usam nome da PF para pedir transferências (Olhar Digital, ago/2025)
77. Polícia de SP faz operação contra golpe do falso policial (Portal Tela, mar/2026)
78. Golpe da agência bancária investigada (Canaltech, cita Febraban)
78. Conheça o golpe da falsa investigação (Olhar Digital)
79. Febraban alerta sobre golpe do falso gerente (Agência Brasil, mar/2026)
80. Criminosos pedem Pix a familiares de pacientes internados (BandNews FM)
80. Falsos médicos aplicam golpes na família de pacientes (Canaltech)
81. Golpes com deepfake e vozes clonadas estão em alta (Canaltech)
81. Clonagem de voz e imagem por IA (Jornal da Band, jan/2026)
82. Acidente que matou família na BR-251 é usado para golpe (Estado de Minas, abr/2026)
82. Golpistas miram serviços funerários em Diadema (Correio da Manhã, fev/2026)
83. Anvisa alerta: famosos e médicos vendendo remédios é golpe com IA (Band)
83. Atores interpretam médicos para vender produtos milagrosos (Correio Braziliense)
84. Principais golpes virtuais com planos de saúde (Folha Vitória)
84. Cartilha alerta para boleto falso de planos de saúde (Jovem Pan)
85. Dona de agência é presa por golpe de falsos pacotes (Mais Goiás)
85. Procon suspende agência suspeita de golpes no ES (Folha Vitória)
86. Procon alerta sobre falsa venda de milhas (Folha BV)

- 87. Booking esclarece golpe que usa dados de reservas (Mercado & Eventos)
- 87. Golpe faz você pagar em dobro pela reserva (Olhar Digital)
- 88. Golpe das milhas usa SMS com link falso (Tecnoblog)
- 88. Phishing usa expiração de pontos como isca (BMC News)
- 89. Golpe do Pix aparece após chuvas em MG e governo faz alerta (TecMundo, 2026)
- 89. Eduardo Leite alerta para golpes em doações no RS (Jovem Pan)
- 90. Centenas de anúncios na Meta promovem falso bolão da Mega da Virada (Aos Fatos)
- 90. Caixa alerta para apostas não autorizadas (NSC Total)
- 91. Golpe no WhatsApp promete passagens grátis (Olhar Digital)
- 92. Sefaz-CE alerta sobre golpes com o programa Sua Nota Tem Valor (COAD)
- 93. E-mails de sextorsão reutilizam senhas vazadas (Malwarebytes, mar/2026)
- 94. Golpe amoroso para roubar criptomoedas em apps de relacionamento (ESET)
- 94. Criminosos estrangeiros usam sites de relacionamento para golpes (SBT News)
- 95. Golpes com criptomoedas (ethereum.org)
- 95. Trezor faz alerta de golpe com suporte falso (Coinspeaker)
- 96. Golpe usa falsa página da Receita e ameaça bloqueio de CPF (Folha Vitória)
- 96. Receita Federal alerta sobre novo golpe do CPF (Mais Goiás, ago/2026)
- 97. PRF alerta sobre uso da sigla em falsas multas (Bem Paraná)
- 98. PF e Febraban deflagram ação contra quem cede contas para golpistas (Gazeta SP)
- 98. Febraban endurece regras contra contas laranja (Movimento Econômico, out/2025)
- 99. Golpe do aluguel falso: caução antes da visita (BandNews FM)
- 99. Golpe do falso aluguel acende alerta em Goiânia (Jornal Opção)
- 100. Aposentada perde quase R\$ 12 mil após achar número falso no buscador (Tupi)
- 100. Golpistas anunciam números falsos de suporte da Microsoft (heise, em alemão)