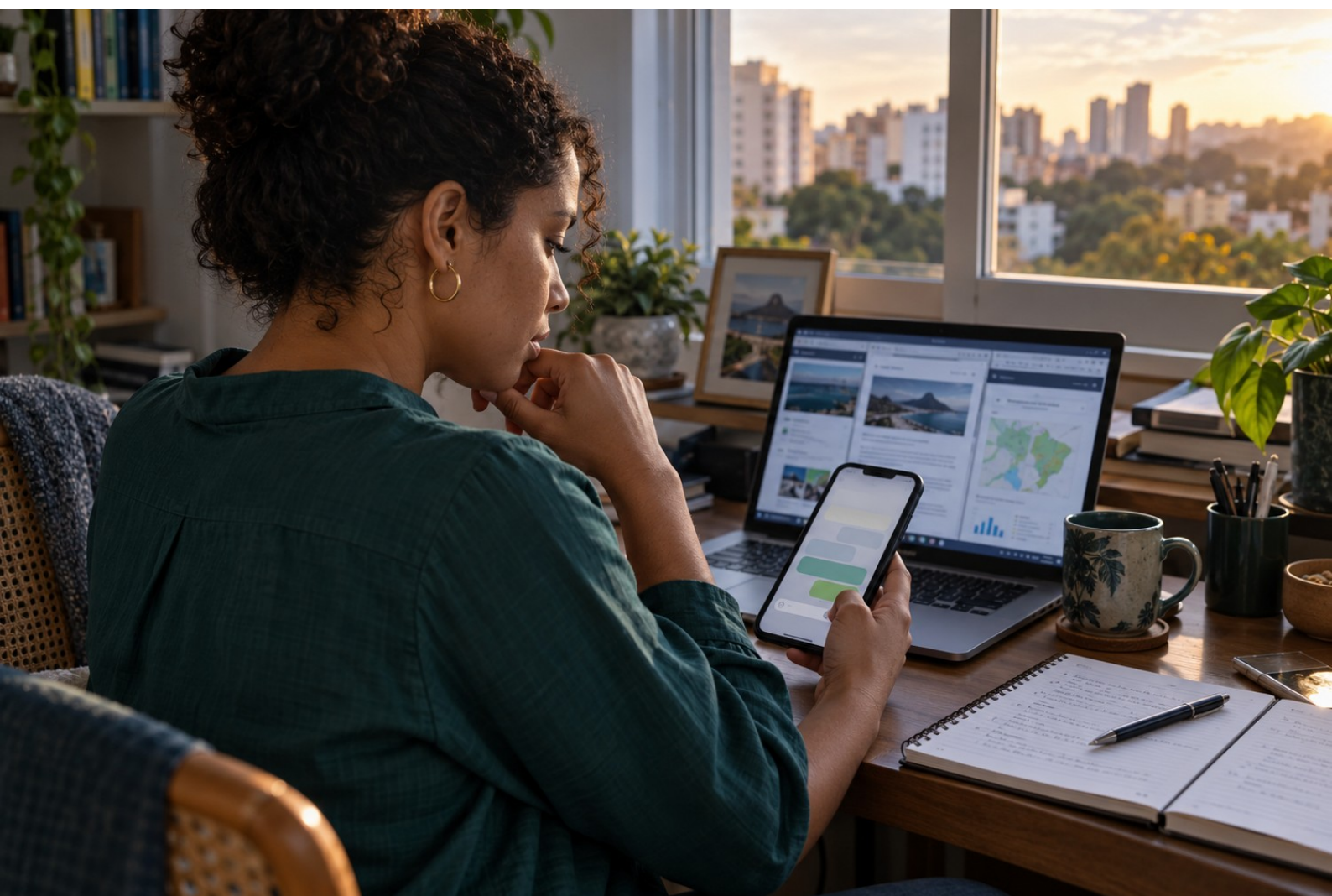


Golpes digitais

como reconhecer e reagir



8

temas para entender
e participar com consciência

Verificação, proteção de contas e primeiros passos diante de uma fraude

Antes de começar

Uma mensagem conhecida pode chegar de uma conta invadida; uma cobrança convincente pode ser falsa. Esta cartilha apresenta cuidados para verificar pedidos, proteger acessos e organizar uma reação quando algo dá errado. A responsabilidade pelo golpe é de quem o pratica. As orientações reduzem exposição, mas não prometem impedir toda fraude ou recuperar valores.

O que você vai encontrar

- 01 A urgência pode ser parte do golpe
- 02 Nome, foto e voz não bastam
- 03 Abra o serviço pelo caminho que você conhece
- 04 Confira antes de confirmar o pagamento
- 05 Proteja o acesso e a recuperação das contas
- 06 Se houve pagamento, procure a instituição rapidamente
- 07 Se houve acesso, reduza a exposição
- 08 Guarde registros e ofereça apoio sem culpar

Os exemplos sem indicação de um caso real são situações didáticas. As explicações resumem regras e práticas; não substituem a consulta à fonte ou orientação para um caso pessoal.

01 A urgência pode ser parte do golpe

Pressão e aparência de autoridade podem encurtar sua verificação.

Pressão	Querem uma ação imediata?
Pedido	Envolve dinheiro, dados ou acesso?
Verificação	Há outro canal confiável?

Golpistas podem combinar medo, oportunidade ou afeto com uma identidade conhecida. Uma mensagem bem escrita, um logotipo ou informações verdadeiras sobre você não comprovam a origem. A tentativa pode ocorrer por ligação, mensagem, anúncio ou conversa prolongada.

Interrompa a sequência antes de pagar ou entregar acesso. Procure a pessoa ou instituição por um canal que você já conhecia, sem usar o contato enviado na própria mensagem. Essa pausa é uma recomendação prática de prevenção, não uma forma de responsabilizar quem foi enganado.

Exemplo hipotético: Uma mensagem informa que o cadastro será bloqueado em minutos. A pessoa abre o aplicativo oficial por conta própria e consulta o atendimento antes de responder.

Separe a pressão para agir da verificação de quem está pedindo.

[Acessar a fonte \[6\]: Golpes: Não se Deixe Enganar — p. 3-12: sinais, pressão e confirmação](#)

02 Nome, foto e voz não bastam

Uma identidade aparente pode ser copiada ou usada sem autorização.

Identidade	Quem afirma estar falando?
Confirmação	Como verificar fora da conversa?
Pedido	A solicitação faz sentido?

Uma conta invadida pode enviar pedidos aos contatos reais da vítima. Fotos e áudios também podem ser reaproveitados ou fabricados. Não use apenas a semelhança da voz ou do perfil como confirmação de identidade, especialmente quando o pedido envolve transferência ou código de acesso.

Confirme por outro meio conhecido e combine procedimentos de verificação em família ou no trabalho. Evite revelar novos dados enquanto tenta confirmar a identidade. Se a conta de alguém foi comprometida, avise por um caminho independente, sem ampliar a circulação do conteúdo fraudulento.

Exemplo hipotético: Um suposto familiar pede uma transferência por um número novo. A pessoa liga para o contato antigo e confirma que o pedido não partiu dele.

Verifique a identidade por um canal independente antes de atender ao pedido.

[Acessar a fonte \[6\]: Golpes: Não se Deixe Enganar — p. 11-12: dados verdadeiros, voz e imagem](#)

03 Abra o serviço pelo caminho que você conhece

Um link ou anúncio pode conduzir a uma página que imita a verdadeira.

Entrada	Como você chegou à página?
Endereço	Qual domínio está aberto?
Instalação	O que querem que você execute?

Mensagens e resultados de busca podem levar a páginas falsas que imitam instituições conhecidas. Aparência e posição na busca não comprovam a origem. Confira o endereço e procure o serviço pelo aplicativo ou caminho oficial que você já conhece.

Para operações sensíveis, abra o aplicativo já instalado ou o endereço oficial conhecido. Não instale programas de acesso remoto a pedido de um contato inesperado. Antes de conceder permissões, verifique a finalidade e a origem. Se houver dúvida, interrompa e procure suporte por um canal independente.

Exemplo hipotético: Uma falsa central pede a instalação de um aplicativo para cancelar uma compra. A pessoa encerra o contato e procura o atendimento no aplicativo do banco.

Entre por um caminho conhecido e desconfie de instalações solicitadas por terceiros.

[Acessar a fonte \[5\]: Golpes: Evite Fraudes — p. 5-9: links e canais oficiais](#) • [Acessar a fonte \[1\]: Golpe de acesso remoto — descrição e prevenção do golpe](#)

04 Confira antes de confirmar o pagamento

O destinatário real importa mais que a imagem do comprovante ou da cobrança.

Cobrança	Qual é a origem?
Destino	Quem receberá o valor?
Conferência	Os dados correspondem ao esperado?

Um boleto, uma chave de pagamento ou um código visual podem ter sido substituídos. Confira os dados apresentados pelo serviço de pagamento antes de confirmar. Uma imagem enviada por mensagem não prova que o dinheiro entrou na sua conta; consulte seu próprio extrato.

Se alguém alegar uma transferência por engano, verifique o recebimento e consulte sua instituição sobre a forma correta de devolução. Não siga instruções para enviar a outra conta sem conferir. Descontos ou ameaças de multa não eliminam a necessidade de validar uma cobrança.

Exemplo hipotético: Uma cobrança de mensalidade chega com dados diferentes dos habituais. A pessoa confirma com a instituição por um contato já conhecido antes de pagar.

Confira cobrança, destinatário e valor na tela final da operação.

[Acessar a fonte \[5\]: Golpes: Evite Fraudes — p. 11-14: dados do pagamento e devolução](#)

05 Proteja o acesso e a recuperação das contas

Uma senha forte precisa de cuidados com a segunda etapa e a recuperação.

Senha	É exclusiva para esta conta?
Confirmação	Há uma segunda etapa?
Recuperação	Os contatos estão atualizados?

Prefira senhas longas e diferentes entre serviços; um gerenciador pode ajudar a guardá-las. Ative a verificação em duas etapas quando disponível. Não entregue códigos recebidos nem aprove solicitações de entrada que você não iniciou, mesmo que a pessoa se apresente como suporte.

Revise também o acesso ao e-mail usado para recuperar outras contas. Guarde códigos de recuperação em local seguro e confira sessões conectadas. Esses cuidados devem acompanhar atualizações de dispositivos e aplicativos. Nenhum recurso isolado torna uma conta invulnerável.

Exemplo hipotético: Uma pessoa recebe um código e uma ligação pedindo que o leia para confirmar um cadastro. Não informa o código e verifica a segurança da conta pelo serviço oficial.

Revise uma conta importante: senha, segunda etapa, sessões e recuperação.

[Acessar a fonte \[3\]: Proteção de contas — p. 4-20: senhas, etapas e recuperação](#)

06

Se houve pagamento, procure a instituição rapidamente

Comunicar e contestar são passos de resposta; reembolso não é automático.

Contato

Use o atendimento oficial

Registro

Identifique a operação

Contestação

Pergunte pelo procedimento aplicável

Se você realizou um pagamento sob suspeita de fraude, procure imediatamente sua instituição pelo canal oficial. Informe o que ocorreu, identifique a transação e guarde o protocolo. Não pague uma nova taxa a quem promete recuperar o valor perdido.

No Pix, o Mecanismo Especial de Devolução atende às hipóteses previstas nas regras do sistema. Não garante restituição e não se aplica a qualquer desacordo comercial. Consulte sua instituição sobre o procedimento vigente e seus prazos; comunique a suspeita sem esperar reunir toda a documentação.

Exemplo hipotético: Após perceber uma transferência fraudulenta, a vítima aciona o atendimento oficial e pergunta como abrir a contestação, guardando o identificador e o protocolo.

Comunique a suspeita sem demora e acompanhe o pedido pelo canal oficial.

[Acessar a fonte \[2\]: Devoluções no Pix — seções 2, 4.2 e 7: fraude e limites](#)

07 Se houve acesso, reduza a exposição

A reação depende do que foi entregue ou executado.

Conta	Senha ou sessão comprometida?
Dispositivo	Houve instalação ou execução?
Contato	Quem precisa ser avisado?

Se entregou uma senha, use um dispositivo confiável para alterá-la e revisar sessões, contatos de recuperação e outros serviços em que ela foi repetida. Se perdeu acesso, siga a recuperação oficial. Avise contatos quando sua conta estiver sendo usada para enviar pedidos falsos.

Se instalou um programa suspeito ou permitiu controle remoto, interrompa o acesso e procure suporte técnico confiável. Não continue operações financeiras em um dispositivo possivelmente comprometido. As ações concretas variam com o incidente; uma troca de senha não remove, por si, um programa malicioso.

Exemplo hipotético: Uma pessoa percebe acessos desconhecidos após instalar um aplicativo. Usa outro dispositivo confiável para procurar suporte e proteger as contas mais importantes.

Identifique o tipo de exposição e busque suporte correspondente.

[Acessar a fonte \[4\]: Golpes: Caiu? Veja o que Fazer — p. 4-14: contas e dispositivos](#) • [Acessar a fonte \[3\]: Proteção de contas — p. 4-20: recuperação e proteção](#)

08 Guarde registros e ofereça apoio sem culpar

Documentação ajuda o atendimento; exposição pública pode causar novos danos.

Evidência

Mensagens, datas e transações

Encaminhamento

Instituição, plataforma e polícia

Cuidado

Não divulgar dados sensíveis

Guarde mensagens, endereços, datas, comprovantes e protocolos sem se colocar novamente em contato com o golpista. Considere registrar a ocorrência e denunciar a conta à plataforma. Os canais e as exigências variam; encaminhe os registros às instituições responsáveis, com cuidado para não expor outras pessoas.

Ao ajudar alguém, evite humilhação e promessas de recuperação. Organize com a vítima uma lista de contas afetadas, comunicações feitas e retornos pendentes. A reação deve interromper o dano e permitir acompanhamento, sem transformar uma experiência de fraude em motivo para isolamento ou vergonha.

Exemplo hipotético: Uma família ajuda a reunir os registros e acompanhar os protocolos. Ao alertar amigos, omite documentos, senhas e dados bancários da vítima.

Monte um registro do incidente e combine o próximo acompanhamento.

[Acessar a fonte \[4\]: Golpes: Caiu? Veja o que Fazer — p. 3-15: atendimento, registros e comunicação](#)

Referências bibliográficas

Fontes em ordem alfabética. Os números identificam os links usados no texto. Os títulos originais e as datas de consulta constam de cada referência.

- [1] BANCO BRADESCO. **Golpe da mão fantasma**. Segurança Bradesco, [s.d.]. Disponível em: <https://seguranca.bradesco/prevencao-de-golpes/golpe-mao-fantasma.html>. Acesso em: 18 out. 2026.
- [2] BANCO CENTRAL DO BRASIL. **Guia de implementação dos procedimentos de devolução no Pix, com ênfase no Mecanismo Especial de Devolução**. Brasília, DF: Banco Central do Brasil, 2026. Versão 4.4. Disposições com vigência em 1 set. e 26 out. 2026; o texto usa apenas fundamentos já vigentes em 18 out. 2026 e não antecipa a alteração futura. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Regulamento_Pix/versoes_futuras/Guia_MED-versao4-4.pdf. Acesso em: 18 out. 2026.
- [3] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Autenticação**. São Paulo: NIC.br, 2022. Cartilha de Segurança para Internet. Data indicada no documento: nov. 2022. Disponível em: <https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf>. Acesso em: 18 out. 2026.
- [4] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Golpes: Caiu? Veja o que Fazer**. São Paulo: NIC.br, 2026. Cartilha de Segurança para Internet. Data indicada no documento: maio 2026. Disponível em: <https://cartilha.cert.br/fasciculos/golpes-o-que-fazer/fasciculo-golpes-o-que-fazer.pdf>. Acesso em: 18 out. 2026.
- [5] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Golpes: Evite Fraudes**. São Paulo: NIC.br, 2026. Cartilha de Segurança para Internet. Data indicada no documento: mar. 2026. Disponível em: <https://cartilha.cert.br/fasciculos/golpes-evite-fraudes/fasciculo-golpes-evite-fraudes.pdf>. Acesso em: 18 out. 2026.
- [6] NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Golpes: Não se Deixe Enganar**. São Paulo: NIC.br, 2026. Cartilha de Segurança para Internet. Data indicada no documento: mar. 2026. Disponível em: <https://cartilha.cert.br/fasciculos/golpes/fasciculo-golpes.pdf>. Acesso em: 18 out. 2026.

Sobre esta cartilha

Para conferir antes de compartilhar

- 1 QUEM ESTÁ ENVOLVIDO?**
Identifique as pessoas, instituições e responsabilidades de cada situação. Um exemplo não descreve todos os integrantes de um grupo nem permite generalizar uma conduta.
- 2 QUE TIPO DE REGISTRO É ESSE?**
Uma lei estabelece regras; uma pesquisa apresenta resultados e limites; uma notícia relata um acontecimento. Exemplos hipotéticos ajudam a explicar uma ideia, mas não comprovam fatos reais.
- 3 QUAL É A AVALIAÇÃO?**
Diferencie o que a fonte documenta da explicação ou recomendação desta cartilha. Confira o contexto, a data e os limites do documento antes de tirar conclusões ou compartilhar.

Sobre a pesquisa e as interpretações

Esta cartilha é um material educativo baseado em pesquisa documental e fontes identificadas. Explicações e orientações de leitura não substituem os documentos citados nem uma análise de cada caso. O objetivo é ajudar o leitor a conferir informações e participar com consciência.

O que esta seleção permite concluir

Golpes e mecanismos de proteção mudam. O roteiro não substitui suporte técnico, atendimento bancário ou análise jurídica. Contestações dependem das regras e das circunstâncias; nenhuma devolução é garantida.

Recorte editorial: 18 de outubro de 2026. Normas, serviços e conhecimentos podem mudar. Confira a fonte indicada antes de aplicar uma orientação.

Organização: Régys Borges da Silveira

1ª edição · Revisão editorial: 18 de outubro de 2026.

Produção com apoio de inteligência artificial (IA). Ilustrações geradas por IA, sem valor documental. Edição distribuída em formato digital; consulte as fontes pelos links do texto e das referências.

Distribuição gratuita, sem cadastro. Materiais de terceiros mantêm suas condições de uso.

[Conheça os demais volumes da coleção](#)

CONTINUE A EXPLORAR

A leitura continua

Conheça os livros de Régys Borges da Silveira e encontre sua próxima leitura.

Explore os livros →

livros.regys.com.br



Lendo no papel?

Aponte a câmera do celular para o QR code. No PDF, toque no botão ou no endereço acima.

Este convite registra apenas a cartilha de origem e uma contagem agregada de acessos, sem identificar você.