



GUIA DE UTILIDADE PÚBLICA • AGOSTO DE 2026

O guia definitivo contra golpes financeiros no Brasil

Os quinze golpes mais aplicados no país, as oito ferramentas oficiais e gratuitas que blindam o seu CPF, os ajustes que transformam o seu celular em um cofre e o que fazer nas primeiras horas se você já caiu.

Por que a Rio Claro escreveu isto

Somos uma gestora de investimentos independente, registrada na CVM, e passamos os dias cuidando do patrimônio dos nossos clientes. Ver um patrimônio evaporar em vinte minutos de ligação é o tipo de coisa que nenhum plano financeiro conserta depois, e não queremos que isso aconteça nem com os nossos clientes nem com ninguém. Foi por isso que escrevemos este guia.

Leia, ative hoje o que der para ativar e compartilhe com quem você mais ama e com quem você se preocupa.
rioclaro.com.br/guiadeseguranca

Antes de pagar, clicar ou instalar, faça **três perguntas**

Golpe bom não parece golpe. O criminoso de hoje chega sabendo o seu nome, o seu CPF, o banco onde você tem conta e às vezes até o número do seu processo. O que ele não consegue fabricar é a sua calma. Estas três perguntas levam três segundos e derrubam a esmagadora maioria das abordagens.

Eu tenho certeza de quem está falando comigo?

01

Nome, foto de perfil, logo do banco e voz não provam nada — todos podem ser copiados, e a voz hoje é clonada com poucos segundos de áudio. A única confirmação que vale é você mesmo iniciar o contato por um número que já conhecia.

Eu estou no canal oficial?

02

Se a conversa começou por uma ligação recebida, uma mensagem, um link ou um anúncio, você não está no canal oficial. Desligue, feche e entre você mesmo pelo aplicativo do banco ou pelo telefone impresso no verso do seu cartão.

Estão me apressando?

03

A pressa é a ferramenta principal do golpista, porque ela impede você de conferir. Nenhuma instituição séria perde a sua conta, o seu processo ou o seu dinheiro porque você pediu para confirmar depois e ligou de volta.

Os quatro sinais que aparecem em quase todo golpe

1

Criam uma urgência

Existe sempre um prazo curto e uma ameaça de perda: a conta será bloqueada, o valor será devolvido ao réu, a promoção acaba em minutos.

2

Pedem algo que ninguém pede

Código recebido por SMS, senha, token, Pix para uma conta de segurança ou a instalação de um aplicativo indicado por eles.

3

Tiram você do canal oficial

A conversa migra para um WhatsApp pessoal, um link encurtado, uma ligação em outro número ou um aplicativo de suporte remoto.

4

Não deixam você conferir

Qualquer tentativa sua de desligar, pesquisar ou falar com outra pessoa é desencorajada com mais pressa ou mais medo.

Um banco de verdade nunca pede senha, código, token, transferência, Pix para conta segura nem instalação de aplicativo por telefone, WhatsApp, SMS ou e-mail. Se pediram qualquer uma dessas coisas, é golpe — sem exceção e sem meio-termo.

O plano que deixa você o mais seguro possível

Comece por aqui. Cada linha abaixo é uma coisa que se faz uma vez e não precisa repetir, e quase todas são gratuitas e levam poucos minutos. Toque em qualquer uma para ver o passo a passo e o endereço oficial, sem sair desta página.

0 de 33 ações concluídas

BLINDAR O CPF 0 de 7

Fecha as portas para abrirem conta, empresa ou empréstimo no seu nome. É a parte que mais protege e a que quase ninguém fez.

- ☐ **Ativei o BC Protege+ para impedir a abertura de contas no meu nome.**

Banco Central 3 minutos Gratuito

Avisa a todo o sistema financeiro que você não quer abrir contas novas neste momento. Toda instituição autorizada é obrigada a consultar esse cadastro antes de abrir uma conta, o que bloqueia a abertura em seu nome por terceiros. Cobre conta corrente, poupança e conta de pagamento pré-paga, além da sua inclusão como titular ou representante em contas de empresas.

O QUE VOCÊ PRECISA TER

Conta gov.br nível prata ou ouro, com verificação em duas etapas ativada.

| Você pode desligar a proteção quando de fato precisar abrir uma conta e religar depois.

- ☐ **Impedi, na Redesim, que o meu CPF entre no quadro societário de empresas.**

Receita Federal 2 minutos Gratuito

Impede que o seu CPF seja incluído no quadro societário de empresas. É o que evita que alguém abra um MEI, uma sociedade ou uma empresa em seu nome e deixe as dívidas para você descobrir depois. Vale para todos os órgãos de registro, incluindo juntas comerciais, cartórios de pessoas jurídicas e a OAB, e para qualquer porte.

O QUE VOCÊ PRECISA TER

Conta gov.br nível bronze para impedir; nível prata para voltar atrás.

| O bloqueio vale para inclusões futuras e não altera as empresas das quais você já participa.

☐ **Consultei o Registrato e reconheci todas as contas, chaves Pix e empréstimos que apareceram.**

Banco Central **5 minutos** **Gratuito**

Mostra tudo o que existe no sistema financeiro ligado ao seu CPF: em quais instituições você tem relacionamento, quais empréstimos e financiamentos estão no seu nome, quais chaves Pix estão cadastradas e quais operações de câmbio foram feitas. É a ferramenta que revela uma conta ou um empréstimo que você nunca abriu.

O QUE VOCÊ PRECISA TER

Conta gov.br nível prata ou ouro.

Vale consultar de tempos em tempos, e não só depois de um susto. Se aparecer algo que você não reconhece, procure imediatamente a instituição indicada e registre a contestação.

☐ **Consultei o Cadastro Pré e não há linha pré-paga desconhecida no meu CPF.**

Operadoras, com aval da Anatel **1 minuto** **Gratuito**

Informa se existem linhas de celular pré-pagas ativas vinculadas ao seu CPF e em quais operadoras. Linha aberta indevidamente no seu nome é matéria-prima para outros golpes, porque serve para receber códigos e validar cadastros.

O QUE VOCÊ PRECISA TER

Basta informar o CPF, sem login.

As operadoras informam a existência da linha, mas não mostram os números, por privacidade. Se aparecer operadora com a qual você não tem relação, procure o atendimento dela e peça o cancelamento.

☐ **Bloqueei a contratação de consignado no Meu INSS, se sou aposentado ou pensionista.**

INSS **3 minutos** **Gratuito**

Impede que qualquer instituição contrate empréstimo consignado descontado do seu benefício enquanto o bloqueio estiver ativo. É a proteção mais eficaz que existe hoje para aposentados e pensionistas. Vale para novos contratos; os já existentes seguem como estão.

O QUE VOCÊ PRECISA TER

Conta gov.br do próprio beneficiário.

Também dá para fazer pelo telefone 135. Para contratar um empréstimo de verdade, basta desbloquear antes e bloquear de novo depois.

☐ **Se aposto, ativei a autoexclusão para bloquear o meu CPF nas casas de apostas.**

Ministério da Fazenda **3 minutos** **Gratuito**

Bloqueia o uso do seu CPF em todas as casas de apostas autorizadas no país, de uma vez só, e interrompe o envio de publicidade dirigida por SMS, e-mail e aplicativo. O efeito alcança todas as plataformas autorizadas em até setenta e duas horas.

O QUE VOCÊ PRECISA TER

Conta gov.br nível prata ou ouro.

Além da proteção financeira, reduz muito o volume de abordagem comercial que serve de disfarce para golpes. Se apostas não fazem parte da sua vida, marque este item e siga adiante.

☐ **A minha conta gov.br está no nível prata ou ouro e com verificação em duas etapas.**

Governo federal

10 minutos

Gratuito

É a conta mais importante que você tem, e quase ninguém a trata assim. É por ela que se acessa o Meu INSS, a Receita Federal, o Registrato e boa parte da sua vida financeira — e é ela que destranca quase tudo o que está nesta lista. Subir de nível é o que libera os serviços mais sensíveis.

- 1 Abra o aplicativo gov.br e veja em que nível a sua conta está: bronze, prata ou ouro.
- 2 Para subir para prata, valide por reconhecimento facial com a base da Justiça Eleitoral ou pelo aplicativo do seu banco credenciado.
- 3 Ative a verificação em duas etapas dentro do próprio aplicativo, na área de segurança da conta.

Nunca informe a senha do gov.br a quem ligar oferecendo ajuda com benefício, restituição ou cadastro. O governo não liga pedindo senha.

BLINDAR O CELULAR 0 de 8

O aparelho é a chave da sua vida financeira. São ajustes gratuitos, feitos uma vez, que mudam o que um criminoso consegue fazer com ele na mão.

☐ **Ativei o PIN do chip, para o meu número não funcionar em outro aparelho.**

2 minutos

Gratuito

Sem essa senha, quem tirar o seu chip e colocar em outro aparelho passa a receber os seus SMS e as suas ligações, inclusive os códigos de confirmação do banco.

- 1 No Android, procure por segurança do chip nas configurações e ative o bloqueio.
 - 2 No iPhone, vá em Ajustes, depois Celular, depois PIN do SIM.
 - 3 Ative usando o PIN padrão da operadora e troque em seguida por um seu, guardado em lugar seguro.
-

☐ **Configurei o aparelho para não mostrar o conteúdo das mensagens com a tela bloqueada.**

1 minuto

Gratuito

Com a tela bloqueada, o aparelho não deve mostrar o texto das mensagens. É nele que aparecem os códigos que o criminoso precisa para tomar as suas contas.

- 1 Nas configurações de notificações, escolha ocultar o conteúdo na tela de bloqueio.
 - 2 Mantenha apenas o aviso de que existe uma mensagem nova, sem o texto dela.
-

☐ **Liguei a proteção contra roubo do Android ou a Proteção de Dispositivo Roubado do iPhone.**

3 minutos

Gratuito

Os dois sistemas passaram a oferecer travas específicas para o momento do roubo, e elas não vêm ligadas em todos os aparelhos.

- 1 No Android, em configurações do Google, ative a proteção contra roubo. Ela bloqueia a tela ao detectar o movimento brusco de arrancada e também quando o aparelho fica muito tempo sem internet.
- 2 No iPhone, em Face ID e Código, ative a Proteção de Dispositivo Roubado. Ela passa a exigir biometria e uma espera de uma hora para mudanças críticas feitas longe dos seus locais habituais.

☐ **Instalei o Celular Seguro e cadastrei uma pessoa de confiança.**

Ministério da Justiça

5 minutos

Gratuito

Permite pedir, em um único lugar, o bloqueio da linha, do aparelho e das contas nas instituições parceiras em caso de roubo, furto ou perda. Também deixa consultar se um aparelho usado tem registro de roubo antes de você comprá-lo. Existe o bloqueio total, que inutiliza o aparelho, e o modo recuperação, que o mantém rastreável pela polícia.

O QUE VOCÊ PRECISA TER

Conta gov.br e o aplicativo instalado antes de precisar.

Cadastre uma pessoa de confiança. É ela quem consegue acionar o bloqueio quando o seu celular está justamente na mão do criminoso.

☐ **Configurei o modo rua ou reduzi os limites de Pix no aplicativo do meu banco.**

5 minutos

Gratuito

Vários bancos deixam você definir um limite pequeno para quando estiver fora das suas redes conhecidas, exigindo reconhecimento facial acima disso.

- 1 Procure por modo rua ou por limites na área de segurança do aplicativo do seu banco.
- 2 Reduza também o limite noturno de Pix. Por regra do Banco Central ele já é limitado para pessoas físicas, mas você pode diminuí-lo ainda mais.

☐ **Nunca instalo aplicativo indicado por quem ligou, e revisei as permissões de acessibilidade.**

3 minutos

Gratuito

É a porta do golpe de acesso remoto, e o fato de o aplicativo existir na loja oficial não significa nada. Uma vez instalado, ele deixa o criminoso ver a sua tela e operar o seu banco enquanto conversa com você ao telefone.

- 1 Desative a instalação de aplicativos de fontes desconhecidas.
- 2 Nas configurações de acessibilidade, revise se algum aplicativo tem permissão que você não reconhece e remova.

☐ **Uso cartão virtual para compras pela internet e recebo notificação de cada compra.**

3 minutos

Gratuito

Cartão virtual para internet reduz o estrago quando os dados vazam, porque você o descarta e gera outro em segundos.

- 1 Gere um cartão virtual no aplicativo do banco para assinaturas e compras pela internet.
- 2 Mantenha o limite baixo e ative as notificações de compra, para ver qualquer lançamento estranho no mesmo dia.

-
- ☐ **Deixei o resgate pronto: localização remota ativa e os telefones do banco e da operadora anotados no papel.**

5 minutos

Gratuito

Depois do roubo você não terá o aparelho para configurar nada, então a preparação precisa acontecer hoje. Este é o item que as pessoas mais adiam e o que mais faz falta na hora.

- 1 Confira se a localização remota está ativa: Buscar iPhone, no iPhone, ou Encontre Meu Dispositivo, no Android.
- 2 Anote em um papel, guardado em casa, o número da central do seu banco e o da sua operadora.
- 3 Guarde também o IMEI do aparelho, que está na nota fiscal e na caixa.

SENHAS E CONTAS 0 de 9

Boa parte dos prejuízos não começa com uma invasão sofisticada, e sim com uma senha anotada onde qualquer um encontra.

- ☐ **Não existe mais nenhuma senha guardada em notas, fotos, contatos ou e-mails.**

10 minutos

Gratuito

Um arquivo chamado senhas, uma foto do papel com a senha do cartão ou um contato salvo com a numeração do cofre são as primeiras coisas que alguém procura em um celular desbloqueado. Apague hoje, mesmo que dê trabalho reconstruir depois.

Apague também da lixeira das notas e do backup na nuvem, onde o arquivo costuma sobreviver por mais trinta dias depois de apagado do aparelho.

- ☐ **Deixei no bloco de notas uma nota chamada senhas, com dados inventados, para confundir quem mexer no meu celular.**

5 minutos

Gratuito

Só depois da ação anterior

Quem rouba um celular desbloqueado procura primeiro por um arquivo chamado senhas, cofre, banco ou cartões. Uma nota com esse nome e conteúdo inventado faz o criminoso perder tempo testando o que não existe — e tempo é exatamente o que separa o prejuízo do bloqueio feito a tempo.

- 1 Confirme antes que as senhas verdadeiras já saíram das notas, das fotos e dos contatos. Sem isso, esta ação não protege nada.
- 2 Crie uma nota com um nome que chame atenção, do tipo senhas do banco.
- 3 Preencha com números plausíveis e falsos, do tipo que exige uma tentativa para se descobrir que não funciona.
- 4 Não use nada parecido com as suas senhas reais, nem uma variação delas.

Isto é uma armadilha, e não uma proteção: ela atrasa o criminoso, e só. A proteção de verdade é a ação anterior desta lista, e é ela que precisa estar feita primeiro.

-
- ☐ **Uso um cofre de senhas, nem que seja o que já vem no aparelho.**

10 minutos

Gratuito

O chaveiro do iPhone e o gerenciador do Google já vêm no aparelho, são gratuitos e guardam tudo criptografado atrás da sua biometria. Com ele, cada site pode ter uma senha diferente sem você precisar decorar nenhuma.

-
- ☐ **As senhas do banco e do e-mail são exclusivas e não se repetem em nenhum outro lugar.**

15 minutos

Gratuito

O e-mail é o mestre de todas as suas contas, porque é por ele que qualquer serviço redefine senha. Quem entra no seu e-mail entra em tudo o mais, em sequência. Essas duas senhas merecem ser exclusivas, longas e não existir em nenhum outro cadastro seu.

-
- ☐ **Ativei a verificação em duas etapas nas contas importantes, de preferência por aplicativo autenticador.**

10 minutos

Gratuito

O SMS depende da sua linha, e a linha pode ser transferida para outro chip. Um aplicativo autenticador gera o código dentro do aparelho, e as chaves de acesso, as passkeys, dispensam senha e usam a sua biometria. Onde o serviço oferecer, prefira essas duas opções ao código por mensagem.

-
- ☐ **Ativei a confirmação em duas etapas do WhatsApp e cadastrei um e-mail de recuperação.**

2 minutos

Gratuito

É um PIN de seis dígitos exigido para registrar a sua conta em qualquer aparelho novo. Sem ele, o código que chega por SMS é a única barreira entre um golpista e a sua lista de contatos inteira.

- 1 No WhatsApp, abra Configurações, depois Conta, depois Confirmação em duas etapas.
- 2 Defina o PIN de seis dígitos e cadastre um e-mail de recuperação, sem o qual você fica sem saída se esquecer o PIN.

-
- ☐ **Apaguei fotos de documentos e selfies com documento da galeria e das conversas.**

10 minutos

Gratuito

Foto de RG, CNH, comprovante de residência e selfie segurando documento são o kit completo para abrir conta no seu nome. Se você precisou enviar algum, apague depois.

Apague também da lixeira da galeria, do backup na nuvem e das conversas em que você enviou. Em muitos aparelhos o arquivo continua por mais trinta dias na lixeira.

☐ **Procurei por senhas nas conversas do WhatsApp e apaguei as mensagens com dados sensíveis.**

15 minutos

Gratuito

Conversa de WhatsApp é o lugar onde as pessoas mandam senha de wi-fi, número de cartão, foto de documento e código de banco, e nunca mais voltam lá. O aplicativo tem busca: use-a contra você mesmo, antes que alguém use.

- 1 Abra a busca do WhatsApp e procure por senha, código, cartão, CVV, PIN, banco, agência, conta, boleto e wifi.
- 2 Confira também as conversas com você mesmo e os grupos de família, onde esse tipo de coisa costuma ser despejado.
- 3 Apague as mensagens que tiverem dado sensível, escolhendo apagar para mim e, quando ainda der, apagar para todos.
- 4 Repita a busca na galeria por fotos de documento e de cartão que tenham chegado por lá.

Apagar para todos só funciona dentro do prazo que o aplicativo permite. Passado o prazo, a mensagem continua no aparelho de quem recebeu, e a única saída é pedir para a pessoa apagar.

☐ **Tranquei o WhatsApp com biometria e deixei a minha foto de perfil visível só para os meus contatos.**

3 minutos

Gratuito

São duas proteções diferentes no mesmo lugar. A tranca impede que alguém com o celular na mão leia as suas conversas, mesmo que a tela esteja desbloqueada. E esconder a foto de perfil de quem não é seu contato tira do criminoso a matéria-prima do golpe do WhatsApp clonado: é com o seu rosto que ele convence a sua mãe.

- 1 Em Configurações, Privacidade, Bloqueio do aplicativo, ative a exigência de biometria para abrir o WhatsApp.
- 2 Ainda em Privacidade, coloque Foto do perfil, Recado e Visto por último como visíveis apenas para Meus contatos.
- 3 Desative a confirmação de leitura se quiser, e revise quem pode adicionar você em grupos, deixando também em Meus contatos.

A foto de perfil é pública por padrão para qualquer pessoa que tenha o seu número, e números vazam às centenas de milhares. É por isso que o golpista consegue montar um perfil idêntico ao seu em minutos.

BLINDAR O PATRIMÔNIO 0 de 3

Os itens acima fecham portas. Estes limitam o estrago se alguma delas ceder: o que um criminoso leva é, no fim, o que você consegue movimentar em minutos.

☐ **A conta que uso no dia a dia não é a mesma onde ficam os meus investimentos.**

30 minutos, uma vez **Gratuito**

É a separação que mais reduz prejuízo em roubo de celular, acesso remoto e coação. A conta do dia a dia é a que está desbloqueada no seu aparelho, com Pix pronto e limite ativo — e é ela que o criminoso alcança. Se o patrimônio mora em outro lugar, com outro acesso, o que ele encontra é o dinheiro do mês, e não a vida inteira.

- 1 Escolha uma instituição para o dia a dia e outra para o patrimônio, e mantenha na primeira apenas o que você usa no mês.
- 2 Use senhas diferentes nas duas, e uma biometria ou segundo fator próprio na conta do patrimônio.
- 3 Não deixe as duas com Pix liberado no mesmo aparelho: a conta do patrimônio não precisa de chave Pix cadastrada.

Vale também para quem tem tudo num banco só: dá para separar em contas distintas dentro da mesma instituição, o que já ajuda, embora separar de fato as instituições ajude mais.

☐ **O que posso resgatar em minutos é só o que eu preciso no curto prazo, e não o meu patrimônio inteiro.**

Uma conversa, não um clique

Todo golpe que termina em transferência tem um teto, e esse teto é o quanto você consegue mover naquele momento. Um patrimônio inteiro disponível para saque imediato transforma vinte minutos de ligação, ou dez de coação na rua, no prejuízo de uma vida. Quando o dinheiro de longo prazo exige um passo a mais — um resgate que leva um dia, uma ordem que você dá em outro canal — esse passo é justamente o tempo que falta ao criminoso, e o tempo que sobra para você desconfiar.

- 1 Calcule quanto você de fato usa por mês e quanto quer ter à mão para imprevisto.
- 2 Verifique quanto do seu patrimônio está hoje resgatável em minutos, somando conta, poupança e aplicações com liquidez imediata.
- 3 Se a segunda conta for muito maior do que a primeira, é aí que está a sua exposição.

Isto não é recomendação de investimento, e nenhum guia genérico pode dizer o que serve para você: o equilíbrio entre ter dinheiro à mão e reduzir exposição depende dos seus objetivos, dos seus prazos e do que você já tem. É uma conversa a se ter com alguém que olhe o seu caso inteiro.

☐ **O aplicativo onde está o meu patrimônio não fica logado e desbloqueado no celular que anda comigo na rua.**

5 minutos **Gratuito**

De nada adianta separar as contas se as duas abrem com o mesmo toque no mesmo aparelho. O acesso ao patrimônio deve exigir alguma coisa que não esteja no bolso junto com o celular.

- 1 Deslogue do aplicativo de investimentos e não marque a opção de manter conectado.
- 2 Exija biometria ou senha própria para abrir esse aplicativo, diferente da que desbloqueia o aparelho.
- 3 Se possível, deixe o segundo fator dessa conta num aparelho ou aplicativo autenticador diferente do celular que você leva na rua.

A maior parte dos golpes que dão certo passa por alguém que não teve com quem conferir. Segurança em casa é combinado, não é aula.

☐ **Combinei uma palavra-código com a minha família para pedidos de dinheiro.**

5 minutos

A defesa mais importante da lista

Escolham juntos uma palavra simples que ninguém de fora conheça e combinem que ela será pedida em qualquer pedido de dinheiro por telefone ou mensagem. É a única defesa que funciona contra voz e rosto clonados por inteligência artificial, porque o criminoso pode copiar a voz do seu filho, mas não tem como adivinhar a palavra.

— Não guarde a palavra no celular. Ela vive na cabeça das pessoas, e só.

☐ **Combinei em casa que nenhum assunto de banco se resolve por WhatsApp ou por ligação recebida.**

5 minutos

Se a regra da casa é que pedido de dinheiro sempre se confirma por ligação para o número antigo, a mensagem urgente perde todo o poder no momento em que chega. A regra vale inclusive quando a mensagem vem da foto e do nome de quem você conhece.

— Deixe combinado que qualquer mensagem estranha pode ser encaminhada para você a qualquer hora, sem cobrança e sem sermão. Medo de passar vergonha é o que faz muita gente pagar calada.

☐ **Tenho o hábito de ler o nome e o CNPJ do beneficiário antes de confirmar qualquer pagamento.**

30 segundos, toda vez

Quase todo prejuízo com pagamento poderia ter sido evitado por uma leitura atenta da tela de confirmação. Ela existe justamente para isso, e é a última porta antes de o dinheiro sair.

- 1 Leia o nome de quem vai receber. Na tela de confirmação do Pix ou do boleto, o banco mostra o nome e o CPF ou CNPJ do beneficiário, e esse nome precisa ser o de quem você realmente deve.
- 2 Estranhe pessoa física no lugar de empresa. Se você ia pagar um condomínio, uma escola ou uma loja e aparece o nome de uma pessoa, pare. Essa conferência sozinha derruba o golpe do boleto trocado.
- 3 Confira o valor e o banco no boleto. O valor aparece no fim da linha digitável e precisa bater com o impresso; os três primeiros números identificam o banco emissor.
- 4 Desconfie de mudança de conta. Aviso de nova conta, nova chave Pix ou segunda via corrigida é o formato preferido do criminoso, e se confirma por voz, no telefone que você já tinha.
- 5 Pague no cartão quando puder. Em compras pela internet o cartão de crédito permite contestar a cobrança; o Pix é imediato e não tem estorno automático.
- 6 Se é você quem vende, deixe o dinheiro cair antes de entregar. Comprovante enviado pelo comprador e Pix agendado não são pagamento.

☐ **Cadastrei os meus telefones no Não Me Perturbe.**

Anatel e bancos

3 minutos

Gratuito

Bloqueia ligações de telemarketing de operadoras e de bancos que oferecem crédito e cartão. Serve à segurança por um motivo indireto e poderoso: quando a oferta legítima por telefone some, qualquer ligação desse tipo passa a ser um sinal de alerta claro.

O QUE VOCÊ PRECISA TER

Apenas o número de telefone que você quer proteger.

O bloqueio leva até trinta dias para entrar em vigor e vale por um ano, então convém renovar. Ligações de cobrança, de prevenção a fraude e de serviços que você contratou continuam chegando.

☐ **Confiro o extrato da conta, do cartão e do benefício pelo menos uma vez por mês.**

10 minutos por mês

O consignado indevido e a assinatura fantasma vivem de passar despercebidos. São valores pequenos, mensais, desenhados para não chamar atenção — e é a conferência de rotina que os encontra enquanto ainda dá para contestar.

Aposentados e pensionistas devem conferir o extrato de pagamento do benefício no Meu INSS, e não apenas o valor que caiu na conta: o desconto aparece lá antes de aparecer aqui.

☐ **Ajudei um familiar mais velho a fazer estas mesmas configurações.**

Meia hora, um domingo

Sentar meia hora com os pais para ativar o PIN do chip, esconder o conteúdo das notificações, ligar a confirmação em duas etapas do WhatsApp e bloquear o consignado vale mais do que qualquer aviso repetido ao telefone.

Conte em casa os golpes que você viu, inclusive os que quase deram certo com você. A conversa banal de hoje é a hesitação salvadora de amanhã.

A lista é longa, e é longa de propósito: preferimos entregar o conjunto completo a entregar só o que é fácil. Quando você tiver marcado tudo, terá fechado praticamente todas as portas que um criminoso usa hoje para chegar ao seu dinheiro. **Segurança absoluta não existe**, e ninguém honesto vai prometer isso a você. O que existe é a diferença enorme entre ter essas portas abertas e tê-las fechadas.

Reconheça a **conversa** antes de reconhecer o golpe

Ninguém identifica um golpe pelo nome técnico dele. Identifica pela frase que acabou de ouvir. Escolha abaixo por onde o golpe costuma chegar até você e toque em qualquer um para ver como ele funciona, o que o criminoso diz e como não cair.

LIGAÇÃO

A falsa central do banco

Ligam avisando de uma compra suspeita no seu cartão e conduzem você, passo a passo, até entregar o dinheiro achando que está protegendo ele.

O QUE ELE DIZ

Identificamos uma compra de R\$ 3.800,00 na sua conta. Foi o senhor que realizou?

Vamos cancelar agora. Só preciso que confirme o código que acabou de chegar.

Para proteger o saldo, transfira para a sua conta segura.

COMO FUNCIONA

Assim que você diz que não reconhece a compra, o criminoso assume o papel de quem está te salvando. A partir daí ele conduz a conversa: pede o código que chegou por SMS, manda entrar no aplicativo, orienta uma transferência para uma suposta conta segura ou pede a instalação de um aplicativo de proteção. Cada passo parece o socorro, e cada passo é o roubo.

COMO NÃO CAIR

- ✓ Desligue o telefone, sem se explicar e sem medo de ser mal-educado.
- ✓ Ligue você mesmo para o número impresso no verso do seu cartão ou use o chat dentro do aplicativo do banco, que você abre digitando o nome, nunca por link.
- ✓ Se a compra existir mesmo, ela continuará lá quando você ligar. Nada se perde por conferir.

O falso gerente ou setor antifraude no WhatsApp

Uma mensagem com a logo do banco, o seu nome completo e dados verdadeiros pede uma atualização cadastral ou uma confirmação de segurança.

O QUE ELE DIZ

Aqui é do setor antifraude do seu banco. Precisamos atualizar seu cadastro hoje.

Me envie a foto do documento para validar a titularidade.

Clique no link e confirme os dados para não ter a conta bloqueada.

COMO FUNCIONA

Os dados que impressionam você — nome completo, CPF, agência, o nome do seu gerente — costumam vir de vazamentos e não provam nada sobre quem está do outro lado. A foto de perfil com a logo do banco é apenas uma imagem que qualquer pessoa coloca no próprio número.

COMO NÃO CAIR

- ✓ Não resolva nenhum assunto bancário por WhatsApp de número desconhecido, nem que ele acerte todos os seus dados.
- ✓ Não envie foto de documento, selfie com documento nem código recebido por SMS.
- ✓ Confirme pelo aplicativo do banco ou pelo telefone oficial se existe mesmo alguma pendência no seu nome.

LIGAÇÃO

O acesso remoto e a mão fantasma

Convencem você a instalar um aplicativo de suporte e passam a ver e controlar a sua tela enquanto você assiste.

O QUE ELE DIZ

Seu celular foi invadido. Vamos instalar o módulo de segurança do banco.

Baixe esse aplicativo, é da própria loja oficial, e aceite as permissões que aparecerem.

Não desligue a ligação enquanto o processo estiver rodando.

COMO FUNCIONA

O aplicativo indicado costuma ser um programa legítimo de acesso remoto, o que faz a vítima baixar a guarda: ele está mesmo na loja oficial. O problema não é o aplicativo, é a permissão de acessibilidade que ele pede. Com ela concedida, o criminoso enxerga a tela, digita no lugar da pessoa e faz transferências pelo aplicativo do banco já aberto e autenticado. Em muitos casos ele também vasculha o aparelho procurando senhas guardadas em notas e fotos.

COMO NÃO CAIR

- ✓ Nunca instale um aplicativo indicado por telefone, WhatsApp, SMS ou e-mail, mesmo que ele exista na loja oficial.
- ✓ Desconfie na hora de qualquer pedido para ativar acessibilidade, espelhamento ou controle do aparelho.
- ✓ Se o aplicativo do banco começar a se mexer sozinho, coloque o celular em modo avião imediatamente e ligue para o banco de outro telefone.

O WhatsApp clonado e o falso parente

Chega uma mensagem de um número desconhecido dizendo que é alguém da família que trocou de número e precisa de um Pix agora.

O QUE ELE DIZ

Oi mãe, troquei de número, salva aqui.

Meu celular quebrou e estou usando o do trabalho.

Preciso de um Pix urgente, depois te devolvo.

COMO FUNCIONA

Existem duas versões. Na primeira, o criminoso apenas usa a foto e o nome do seu parente em outro número. Na segunda, ele realmente tomou a conta dele: convenceu a vítima a repassar o código de seis dígitos que chega por SMS e passou a escrever de dentro do WhatsApp verdadeiro, com o histórico e os contatos à mão.

COMO NÃO CAIR

- ✓ Nunca repasse o código de seis dígitos que chega por SMS, nem para alguém que se apresente como suporte do WhatsApp.
- ✓ Antes de qualquer Pix, ligue para o número antigo da pessoa ou faça uma chamada de vídeo. O criminoso desconversa.
- ✓ Ative a confirmação em duas etapas do WhatsApp, que exige um PIN próprio para registrar a conta em outro aparelho.

LIGAÇÃO

A voz e o rosto clonados por inteligência artificial

A ligação tem mesmo a voz do seu filho, e a chamada de vídeo tem mesmo o rosto dele. Nada disso prova mais nada.

O QUE ELE DIZ

Mãe, sou eu, me aconteceu uma coisa e eu não posso falar muito.

Estou com o telefone de outra pessoa, faz esse Pix pra mim que depois eu explico.

COMO FUNCIONA

Poucos segundos de áudio publicados numa rede social bastam para reproduzir o timbre e a entonação de alguém, e o mesmo já vale para o rosto em chamadas de vídeo curtas. O golpe combina a semelhança com uma emergência que impede perguntas: um acidente, uma dívida, um sequestro simulado.

COMO NÃO CAIR

- ✓ Combine com a sua família uma palavra-código, simples de lembrar e que ninguém de fora conheça, e peça essa palavra em todo pedido de dinheiro por telefone.
- ✓ Desligue e ligue você mesmo para o número que você já tinha salvo.
- ✓ Faça uma pergunta cuja resposta só a pessoa real saberia e que não esteja em nenhuma rede social.

O falso advogado e o processo que foi liberado

Usam o nome do escritório, o número real do seu processo e a notícia que você mais quer ouvir para cobrar uma taxa.

O QUE ELE DIZ

Boa notícia: o valor do seu processo foi liberado.

Para receber, é preciso quitar a guia de custas hoje.

Se o pagamento não sair até amanhã, o valor volta para o tribunal.

COMO FUNCIONA

Processos judiciais são públicos, e é daí que saem o número, as partes e o nome do advogado. Com esses dados, a mensagem soa verdadeira. O que não existe é a taxa: nenhum valor de processo depende de um pagamento feito por você a uma conta indicada por WhatsApp.

COMO NÃO CAIR

- ✓ Ligue para o escritório pelo número que você já usava antes, e não pelo número que mandou a mensagem.
- ✓ Desconfie de qualquer cobrança de guia, custas ou honorários que apareça primeiro por mensagem.
- ✓ Confira o andamento diretamente no site do tribunal, que é público e gratuito.

PAGAMENTOS

O boleto falso e o Pix com beneficiário trocado

O documento parece idêntico ao verdadeiro, mas o dinheiro entra na conta de outra pessoa.

O QUE ELE DIZ

Segue o boleto atualizado do condomínio, o anterior teve um erro.

Houve uma mudança na nossa conta, o Pix agora é para esta chave.

COMO FUNCIONA

Acontece com condomínio, escola, IPTU, financiamento, plano de saúde, cartório, obra, viagem e hospedagem. Às vezes o criminoso invadiu o e-mail de quem cobra e reenviou o mesmo documento com os dados de recebimento trocados, o que torna a mensagem convincente até no assunto e na assinatura.

COMO NÃO CAIR

- ✓ Antes de confirmar, leia na tela do seu banco o nome e o CNPJ de quem vai receber. Eles precisam ser exatamente os de quem você deve.
- ✓ Se você deveria pagar uma empresa e aparece o nome de uma pessoa física, pare imediatamente.
- ✓ Diante de qualquer aviso de mudança de conta ou de chave Pix, ligue para o número que você já conhecia e confirme por voz.

PAGAMENTOS

O comprovante falso e o Pix agendado

Mostram o print do pagamento e pressionam para levar o produto embora antes que você confira a conta.

O QUE ELE DIZ

Já mandei o Pix, olha o comprovante aqui.

Deve estar demorando para cair por causa do horário.

COMO FUNCIONA

O print pode ser editado, e o Pix agendado aparece com cara de pagamento feito mesmo antes de sair da conta — e pode ser cancelado depois. Em ambos os casos, quem entrega o produto fica sem o produto e sem o dinheiro.

COMO NÃO CAIR

- ✓ Só entregue o produto depois de ver o valor no extrato da sua própria conta, e não no comprovante enviado pelo comprador.
- ✓ Lembre que print não é pagamento e que agendamento não é pagamento.
- ✓ Se houver pressa incomum para retirar a mercadoria, trate a pressa como o sinal de alerta que ela é.

A loja falsa e a promoção boa demais

Site bonito, preço muito abaixo do mercado, desconto extra no Pix e um relógio correndo na tela.

O QUE ELE DIZ

Últimas unidades com 70% de desconto, só hoje.

No Pix o desconto é ainda maior e a entrega é imediata.

COMO FUNCIONA

O desconto irreal existe para atropelar a sua conferência, e o pagamento no Pix existe porque ele é imediato e difícil de reverter. Muitos desses sites têm poucos dias de vida: eles saem do ar assim que as reclamações aparecem e voltam com outro endereço.

COMO NÃO CAIR

- ✓ Procure o CNPJ no rodapé do site e confirme na Receita Federal se a empresa existe, está ativa e tem a mesma razão social.
- ✓ Leia o nome do domínio com atenção, porque o golpe costuma ser uma letra trocada ou uma palavra a mais no endereço de uma marca conhecida.
- ✓ Prefira pagar com cartão de crédito, que permite contestação, em vez de Pix, que não permite.
- ✓ Pesquise a reputação da loja e desconfie de site sem histórico, sem endereço físico e sem telefone.

A passagem, o hotel e as milhas com desconto irreal

Prometem emissão barata, upgrade garantido ou pacote imperdível, e entregam um localizador que não existe.

O QUE ELE DIZ

Consigo emitir com milhas por metade do preço, só preciso do Pix agora.

Reserva confirmada, segue o print do localizador.

COMO FUNCIONA

A reserva não é o bilhete. Existe uma janela entre reservar e emitir na qual tudo parece certo, e é nessa janela que o criminoso desaparece. Em outros casos, o bilhete é emitido com milhas obtidas em contas invadidas e cancelado pela companhia depois.

COMO NÃO CAIR

- ✓ Consulte o localizador diretamente no site ou no aplicativo da companhia aérea ou do hotel, digitando o endereço você mesmo.
- ✓ Entenda que reserva não é bilhete emitido e que print não é comprovação de nada.
- ✓ Compre com cartão de crédito e no canal oficial, mesmo que saia um pouco mais caro.

O investimento milagroso e o grupo VIP

Prometem lucro alto, fixo e sem risco, normalmente com um robô, uma criptomoeda ou um grupo fechado.

O QUE ELE DIZ

Rendimento garantido de 5% ao mês, sem risco nenhum.

É um grupo fechado, as vagas fecham hoje à noite.

COMO FUNCIONA

Retorno alto, rápido e garantido não existe: onde há retorno maior, há risco maior, e quem promete o contrário está mentindo ou pagando os primeiros com o dinheiro dos últimos. O grupo fechado e o prazo curto existem para impedir que você pesquise e para que a conversa aconteça longe de qualquer registro.

COMO NÃO CAIR

- ✓ Confira se a empresa e a pessoa que oferecem estão autorizadas, consultando a Comissão de Valores Mobiliários e o Banco Central, e veja se o nome aparece na lista de alerta da CVM.
- ✓ Confira se os dados de contato batem exatamente com os do cadastro oficial, porque é comum o criminoso usar o nome de uma instituição verdadeira.
- ✓ Trate a promessa de ganho garantido como o próprio anúncio do golpe.

A criptomoeda travada esperando uma taxa

Avisam que existe uma fortuna em criptomoeda no seu nome, parada e prestes a ser perdida, e que basta pagar uma taxa pequena para liberar tudo.

O QUE ELE DIZ

Sua conta de mineração está inativa há onze meses. Você tem 0,74 BTC acumulados que serão redistribuídos se não houver saque.

O saque foi aprovado. Falta apenas a taxa de liberação de R\$ 890 para o valor cair na sua conta.

A Receita exige o recolhimento antecipado do imposto para desbloquear a transferência.

COMO FUNCIONA

O golpe chega de duas formas. Na primeira, você recebe do nada um aviso de que existe uma carteira antiga, uma conta de mineração esquecida ou uma herança em criptomoeda no seu nome, com um valor alto e um prazo curto antes de o dinheiro ser perdido. Na segunda, você já investiu em uma corretora que parecia real, viu o saldo crescer na tela e agora não consegue sacar. Nos dois casos a conversa termina igual: para liberar, é preciso pagar antes uma taxa, um imposto, uma auditoria ou um seguro. Você paga, e aparece a taxa seguinte. O saldo na tela é apenas um número digitado por eles, e cada pagamento é a única transferência real que existe nessa história.

COMO NÃO CAIR

- ✓ Nenhuma corretora, banco ou plataforma legítima cobra taxa para entregar o dinheiro que já é seu. Imposto se paga sobre lucro realizado, na declaração, e nunca como condição para sacar.
- ✓ Dinheiro que aparece do nada não existe. Se você nunca abriu conta de mineração, não há saldo esquecido a resgatar.
- ✓ Antes de qualquer aporte, confira se a plataforma está autorizada pela Comissão de Valores Mobiliários e pelo Banco Central, e procure o nome na lista de alerta da CVM.
- ✓ Se você já pagou uma taxa, pare imediatamente e não pague a próxima. A partir daqui, cada valor novo é prejuízo adicional garantido, e o caminho é o banco, o MED e o boletim de ocorrência.

O falso empréstimo e a falsa negociação de dívida

Oferecem crédito fácil ou um desconto enorme na dívida, mas exigem uma taxa antes de liberar qualquer coisa.

O QUE ELE DIZ

Seu crédito está pré-aprovado, falta só o pagamento do seguro para liberar.

Consegui um acordo com 90% de desconto, mas precisa pagar a entrada hoje.

COMO FUNCIONA

O golpe se alimenta de quem está apertado e por isso aceita correr um risco. A taxa muda de nome — seguro, tarifa, IOF, custas, entrada do acordo — mas a estrutura é sempre a mesma: você paga primeiro e o dinheiro prometido nunca chega.

COMO NÃO CAIR

- ✓ Saiba que instituição autorizada não cobra pagamento antecipado para liberar empréstimo. O custo é descontado do valor liberado ou embutido nas parcelas.
- ✓ Negocie dívida apenas nos canais oficiais do próprio credor, procurados por você.
- ✓ Confirme no Banco Central se a instituição que ofereceu o crédito é autorizada a funcionar.

O empréstimo consignado que ninguém pediu

Aparece um desconto novo na aposentadoria ou no salário, referente a um contrato que a pessoa nunca assinou.

O QUE ELE DIZ

É só uma confirmação de dados do seu benefício, a senhora faz o reconhecimento facial aqui.

O senhor tem uma margem liberada, é dinheiro que já é seu.

COMO FUNCIONA

O criminoso obtém os dados do benefício e contrata o empréstimo em nome da vítima, às vezes com a ajuda de uma selfie ou de um reconhecimento facial que ele mesmo pediu durante a ligação. O desconto começa a aparecer nos meses seguintes, e quem descobre tarde já pagou várias parcelas.

COMO NÃO CAIR

- ✓ Aposentados e pensionistas podem bloquear preventivamente a contratação de consignado no Meu INSS ou pelo telefone 135, e desbloquear apenas quando realmente forem contratar.
- ✓ Confira o extrato do benefício e do salário todo mês, procurando descontos novos.
- ✓ Nunca faça reconhecimento facial nem envie selfie a pedido de alguém que ligou para você.

O celular roubado que vira a sua conta bancária

O prejuízo raramente é o aparelho. É o que o criminoso faz nos primeiros minutos com ele desbloqueado.

O QUE ELE DIZ

O roubo costuma acontecer com o celular já aberto na mão da vítima, na saída do metrô ou do restaurante.

COMO FUNCIONA

Com o aparelho desbloqueado, o criminoso troca a senha da conta do sistema para impedir o bloqueio remoto, abre os aplicativos de banco, tenta redefinir senhas usando o e-mail e o SMS que chegam ali mesmo, procura fotos de documentos na galeria e senhas anotadas nas notas. Se o chip não tiver PIN, ele coloca o seu número em outro aparelho e passa a receber os seus códigos.

COMO NÃO CAIR

- ✓ Ative o PIN do chip, para que o seu número não funcione em outro aparelho sem a senha.
- ✓ Configure o celular para não mostrar o conteúdo das notificações com a tela bloqueada, porque é ali que aparecem os códigos.
- ✓ Cadastre-se no Celular Seguro e indique uma pessoa de confiança antes de precisar, para que o bloqueio possa ser pedido mesmo sem o aparelho na mão.
- ✓ Use o modo rua ou os limites reduzidos do aplicativo do banco quando estiver fora de casa.

O falso motoboy e a troca do cartão

Depois de uma ligação sobre uma compra suspeita, alguém aparece na sua porta para buscar o cartão.

O QUE ELE DIZ

Vamos enviar um portador para recolher o cartão clonado, deixe ele cortado no envelope.

Antes, digite a senha atual no telefone para nós cancelarmos.

COMO FUNCIONA

É a continuação presencial do golpe da falsa central. A senha é capturada por telefone e o cartão é entregue na mão do criminoso, às vezes trocado por outro parecido para que a vítima demore a perceber. Nenhum banco no Brasil envia alguém à casa do cliente para recolher cartão.

COMO NÃO CAIR

- ✓ Nenhum banco busca cartão na sua casa. Se alguém for, é golpe, e você pode chamar a polícia.
- ✓ Nunca digite nem diga a sua senha durante uma ligação, seja qual for a justificativa.
- ✓ Se precisar cancelar um cartão, corte o chip e a tarja você mesmo e descarte, depois de cancelar pelo aplicativo.

Caí no golpe. E **agora?**

A primeira hora vale mais do que todas as outras juntas, porque o dinheiro ainda pode estar parado na conta de destino. Siga a ordem abaixo e não perca tempo se culpando: isso acontece com gente atenta, informada e experiente todos os dias.

1

NOS PRIMEIROS MINUTOS

Ligue para o banco e peça o bloqueio do valor

Use o telefone do verso do cartão ou o chat de dentro do aplicativo. Diga com todas as letras que você caiu em um golpe e que quer a devolução do Pix. O procedimento se chama Mecanismo Especial de Devolução, o MED, e nem todo atendente conhece a sigla, então descreva o que aconteceu. Anote o número do protocolo.

2

AINDA NO MESMO DIA

Feche as portas que ficaram abertas

Troque as senhas do banco, do e-mail e do gov.br, encerre as sessões abertas em outros aparelhos e revise os dispositivos conectados. Se instalou algum aplicativo durante a conversa, desinstale e reinicie o aparelho. Avise a sua família e o seu trabalho, porque o criminoso costuma usar a sua conta para abordar os seus contatos.

3

NAS PRIMEIRAS 24 HORAS

Registre o boletim de ocorrência

O registro pode ser feito pela internet, na delegacia virtual do seu estado, e tem a mesma validade do presencial. Descreva a data, a hora, o valor, a chave Pix de destino e anexe as conversas. Sem esse documento, tanto a investigação quanto qualquer discussão futura com o banco ficam muito mais difíceis.

4

SE O CELULAR FOI LEVADO

Bloqueie linha, aparelho e contas

Acione o Celular Seguro ou peça que a sua pessoa de confiança acione, ligue para a operadora e bloqueie o chip, e use a localização remota para bloquear e apagar o aparelho. Depois disso, peça o bloqueio do aparelho pelo IMEI, que consta na nota fiscal.

5

NA SEMANA SEGUINTE

Veja o que abriram no seu nome

Consulte o Registrato para procurar contas, chaves Pix e empréstimos que você não reconhece, confira a Redesim e o Cadastro Pré e, aproveitando o susto, ative o BC Protege+ e o bloqueio de consignado se ainda não tiver ativado.

6

SE O BANCO NÃO RESOLVER

Escale por escrito

Procure a ouvidoria da instituição, registre a reclamação no consumidor.gov.br, que é o canal oficial do governo, e leve o caso ao Banco Central ou ao Procon. Guarde todos os protocolos: é o conjunto deles que sustenta o seu caso.

O que as pessoas mais perguntam

Recebi uma ligação que sabia meu nome, meu CPF e até meu gerente. Não pode ser do banco mesmo?

Não pode, se pediram qualquer ação sua. Dados pessoais circulam em vazamentos há anos e são justamente o que dá credibilidade à abordagem. O que separa o banco do criminoso não é o quanto ele sabe sobre você, e sim o que ele pede: nenhuma instituição pede senha, código, token, transferência ou instalação de aplicativo por telefone. Desligue e ligue você mesmo para o número do verso do cartão.

Fiz um Pix para um golpista. Ainda dá para recuperar o dinheiro?

Existe uma chance real, e ela depende de velocidade. O Banco Central criou o Mecanismo Especial de Devolução, que permite ao seu banco pedir o bloqueio e a devolução do valor. O prazo formal para abrir o pedido é de até oitenta dias contados da transação, mas a chance de o dinheiro ainda estar parado na conta de destino é muito maior nas primeiras horas.

Ligue imediatamente para o banco, diga que caiu em um golpe, peça a devolução, anote o protocolo e registre o boletim de ocorrência no mesmo dia.

O BC Protege+ vai me impedir de abrir uma conta quando eu precisar?

Vai, e é exatamente esse o objetivo. A diferença é que você desliga a proteção quando quiser, abre a conta e liga de novo depois. O serviço é gratuito, o efeito é imediato e o histórico de ativações fica visível para você dentro do Meu BC.

Guardar as senhas no navegador ou no celular é seguro?

É bem mais seguro do que anotar em uma nota, em uma foto ou em um papel na carteira, porque o cofre do aparelho guarda tudo criptografado atrás da sua biometria. O risco a evitar é outro: usar a mesma senha em vários serviços. Com um cofre, cada cadastro pode ter a sua própria senha sem que você precise decorar nenhuma.

Aquela ideia de deixar senhas falsas no bloco de notas funciona?

Ela atrapalha um pouco quem revista o aparelho às pressas, e alguns minutos podem fazer diferença. Mas é uma tática, não uma proteção: se as senhas verdadeiras continuam salvas em outro arquivo, em uma foto ou no histórico do e-mail, a isca não serve para nada. O passo que realmente muda o resultado é remover as senhas verdadeiras do aparelho e passar a usar um cofre.

Por que colocar PIN no chip, se o celular já tem senha e biometria?

Porque o chip é retirado do aparelho em segundos e colocado em outro. Sem PIN, o criminoso passa a receber os seus SMS e as suas ligações, e é com esses códigos que ele redefine senhas e entra nas suas contas. O PIN é pedido apenas quando o chip é ligado em um aparelho novo, então ele não atrapalha o seu dia a dia.

Meus pais são idosos e não vão configurar nada disso sozinhos. Por onde começar?

Comece pelas quatro medidas de maior efeito e faça você mesmo, sentado ao lado deles: bloquear o consignado no Meu INSS, ativar a confirmação em duas etapas do WhatsApp, colocar PIN no chip e esconder o conteúdo das notificações na tela bloqueada.

Depois disso, combine a palavra-código da família e deixe claro que eles podem encaminhar qualquer mensagem estranha para você a qualquer hora, sem cobrança. O medo de passar vergonha é o que faz muita gente pagar calada.

Recebi um boleto por e-mail de uma empresa com quem eu realmente tenho contrato. Como confiro?

Antes de pagar, digite a linha digitável no aplicativo do seu banco e leia o nome e o CNPJ do beneficiário que aparecem na tela de confirmação. Eles precisam ser exatamente os de quem você deve. Se aparecer o nome de uma pessoa física no lugar da empresa, pare. Na dúvida, ligue para a empresa pelo telefone que você já usava e peça a segunda via pelo portal dela.

Esse guia serve para empresas também?

A maior parte dele sim, especialmente a conferência antes de pagar, a blindagem do CPF dos sócios e as regras sobre senhas. Empresas têm ainda duas exposições próprias que valem atenção: o e-mail invadido do setor financeiro, usado para reenviar boletos com dados trocados, e a validação de mudanças de conta de fornecedores, que deveria sempre passar por uma confirmação por voz em um número já conhecido.

De onde vem cada informação deste guia 13 fontes oficiais

BC Protege+ e Registrato

— <https://www.bcb.gov.br/meubc>

Banco Central do Brasil

Proteção do CPF no CNPJ

— <https://www.gov.br/pt-br/servicos/impedir-permitir-participacao-do-meu-cpf-no-cadastro-nacional-de-pessoas-juridicas-cnpj>

Receita Federal e Redesim

Programa Celular Seguro

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

Ministério da Justiça e Segurança Pública

Plataforma centralizada de autoexclusão de apostas

— <https://www.gov.br/pt-br/servicos/plataforma-centralizada-de-autoexclusao-apostas>

Ministério da Fazenda

Bloqueio de empréstimo consignado

— <https://www.gov.br/inss/pt-br/noticias/veja-como-bloquear-ou-desbloquear-o-beneficio-para-emprestimo-consignado>

INSS

Consulta de linhas pré-pagas por CPF

— <https://cadastropre.com.br/>

Operadoras participantes, com aval da Anatel

Bloqueio de telemarketing

— <https://www.naomeperturbe.com.br/>

Anatel e instituições financeiras

Consulta de instituições autorizadas

— <https://www.gov.br/pt-br/servicos/consultar-instituicoes-autorizadas-pelo-banco-central>

Banco Central do Brasil

Consulta de participantes autorizados e lista de alerta

— https://www.gov.br/cvm/pt-br/canais_atendimento/consultas-reclamacoes-denuncias/participantes-autorizados

Comissão de Valores Mobiliários

Registro de ocorrência policial pela internet

— <https://www.gov.br/pt-br/servicos/registrar-ocorrencia-policial-online>

Ministério da Justiça e Segurança Pública

Reclamação formal contra instituição

— <https://www.consumidor.gov.br/>

Consumidor.gov.br

Consulta de CNPJ

— https://solucoes.receita.fazenda.gov.br/servicos/cnpjreva/cnpjreva_solicitacao.asp

Receita Federal

Dados sobre golpes de Pix e boleto no Brasil

— <https://portal.febraban.org.br/>

Febraban

Todos os serviços citados são gratuitos e a Rio Claro não tem relação comercial com nenhum deles. Prazos, níveis de conta e endereços mudam: este guia foi revisado em agosto de 2026 e vale conferir na página oficial de cada serviço antes de agir.

Segurança é o primeiro passo do **cuidado com o dinheiro**

O plano termina numa pergunta que nenhum guia genérico consegue responder por você: quanto do seu patrimônio precisa mesmo estar à mão, e quanto poderia estar menos exposto. A resposta depende dos seus objetivos, dos seus prazos e do que você já construiu.

A Rio Claro é uma gestora de investimentos independente, registrada na CVM. Não vendemos produto e não temos meta de banco: primeiro olhamos para a sua vida e para os seus objetivos, e só depois para o mercado. A primeira conversa com um planejador é gratuita e serve justamente para entender a sua situação.

SITE

rioclaro.com.br

E-MAIL

atendimento@rioclaro.com.br

SÃO PAULO

R. Joaquim Floriano, 72 · Itaim Bibi

TELEFONE

(61) 3044-7780

ESTE GUIA

rioclaro.com.br/guiadeseguranca

BRASÍLIA

SCN QD 5, Bloco A, Sala 1208 · Asa Norte

Rio Claro Investimentos · CNPJ 31.249.802/0001-63 · Administradora de carteiras de valores mobiliários registrada na CVM. Aderente à autorregulação da ANBIMA. Este material tem caráter educativo e não constitui recomendação de investimento. As ferramentas oficiais citadas são gratuitas e a Rio Claro não tem relação comercial com nenhuma delas. Guia revisado em agosto de 2026: confirme prazos e endereços na página oficial de cada serviço antes de agir.