

DICAS DE SEGURANÇA

Conta bancária invadida pelo celular: como acontece, como evitar e o que fazer

A pessoa abre o aplicativo do banco e encontra Pix que não fez, empréstimo que não pediu ou o saldo zerado. Na maioria dos casos o banco não foi invadido: o golpista entrou pelo celular da vítima, ou convenceu a vítima a abrir a porta para ele. Este guia mostra os cinco caminhos mais usados contra quem tem Android, como fechar cada um deles e o que fazer nas primeiras horas, que são as mais importantes.

Guia da JAL Softwares e da Vortex CyberSegurança. Atualizado em 20/10/2026.

PARTE 1



Como os golpistas entram na conta

1

Aplicativo malicioso instalado por link.

Chega pelo WhatsApp, SMS ou e-mail, disfarçado de atualização do banco, rastreio de encomenda, benefício do governo ou cupom. É instalado fora da Play Store e pede a permissão de Acessibilidade. Com ela, lê tudo o que aparece na tela, vê a senha sendo digitada e faz Pix sozinho, muitas vezes com a tela escura ou com um aviso falso de "atualizando" para a vítima não perceber. É o caminho mais comum no Brasil.

O QUE É

É o trojan bancário do Android: um aplicativo falso, com cara de útil, feito para roubar a conta do banco. Ele é instalado a partir de um arquivo baixado fora da Play Store, o

APK, e, depois de receber a permissão de Acessibilidade, passa a enxergar e a mexer em tudo o que aparece na tela.

COMO ACONTECE

Chega uma mensagem com link: "atualize o aplicativo do banco", "sua encomenda está retida", "você tem um benefício para receber", "ganhe um cupom". O link baixa o arquivo, o Android avisa que a instalação vem de fonte desconhecida e o próprio golpe explica como liberar.

Instalado, o aplicativo pede a Acessibilidade com uma desculpa, como "para funcionar corretamente". A partir daí ele lê a tela, captura a senha enquanto ela é digitada, abre o banco e faz o Pix sozinho. Para a vítima não perceber, escurece a tela ou mostra um aviso falso de "atualizando, não desligue o aparelho".

COMO SE PROTEGER

- Instale aplicativos só pela Play Store e confira se o desenvolvedor é o banco verdadeiro.
- Nunca libere "instalar apps desconhecidos" porque uma mensagem pediu. A opção fica em Configurações, Apps, Acesso especial, Instalar apps desconhecidos, e muda de nome conforme a marca do celular.
- Desconfie de qualquer aplicativo que peça Acessibilidade sem ser, de verdade, um aplicativo de acessibilidade.
- Deixe o Google Play Protect ligado: ele confere também os aplicativos instalados fora da loja.

O QUE FAZER

1. Desligue a internet do celular, o Wi-Fi e os dados móveis, para cortar o controle do golpista.
2. De outro telefone, ligue para o banco pelo número oficial e peça o bloqueio da conta, do cartão e do Pix.
3. Peça o MED para cada Pix que você não fez.
4. Não fique só em apagar o aplicativo: siga a parte "Depois, no celular: formatar é obrigatório" deste guia.

2

Falsa central do banco, o golpe da mão fantasma.

Alguém liga ou manda mensagem dizendo ser do banco, fala de uma compra suspeita ou de um acesso estranho e pede para a vítima instalar um aplicativo de "segurança" ou de "suporte". Na verdade é um aplicativo de acesso remoto, e a partir daí o golpista controla o celular a distância, como se tivesse uma mão invisível mexendo na tela.

O QUE É

É um golpe de conversa: o golpista não invade nada sozinho, ele convence a vítima a entregar o controle do celular. O nome "mão fantasma" vem do que a vítima vê depois: a tela mexendo sozinha, como se uma mão invisível tocasse nela.

COMO ACONTECE

A ligação parece real. O número pode aparecer como o do banco, o atendente sabe o nome e parte do CPF da vítima, fala de uma compra suspeita ou de um acesso de outro estado e cria urgência. Depois pede para instalar um aplicativo de "segurança", "proteção" ou "suporte".

Esse é o app de acesso remoto do golpe. Programas como AnyDesk, TeamViewer e RustDesk são legítimos e usados por empresas de suporte, mas nas mãos do golpista mostram a tela e permitem tocar nela a distância. Com o controle, ele abre o banco enquanto a vítima ainda está na linha, ou pede que ela digite a senha "para confirmar a identidade".

COMO SE PROTEGER

- Banco não liga pedindo para instalar aplicativo, informar senha, código ou token, nem para fazer Pix de teste.
- Desligue e ligue você mesmo para o número atrás do cartão ou do aplicativo, de outro telefone se possível.
- Não instale aplicativo durante uma ligação, por mais convincente que seja o atendente.
- Não confie no número que aparece na tela: ele pode ser falsificado para parecer o do banco.

O QUE FAZER

1. Desligue a ligação e desligue a internet do celular.
2. De outro telefone, ligue para o banco pelo número oficial e peça o bloqueio de tudo.
3. Peça o MED para cada Pix feito sem você e registre o boletim de ocorrência, com o número que ligou.
4. Formate o celular: com o acesso remoto, o golpista pode ter instalado outros aplicativos.

3

Site ou mensagem falsa do banco.

Um link leva para uma página igual à do banco, que pede agência, conta, senha, token ou foto do rosto. Com esses dados, o golpista entra na conta pelo aparelho dele.

O QUE É

É o phishing: uma página falsa, muito parecida com a do banco, feita só para capturar os dados de quem digita. Aqui o celular da vítima nem precisa estar infectado, porque o golpista usa os dados no aparelho dele.

COMO ACONTECE

O link chega por SMS, e-mail, WhatsApp ou anúncio patrocinado no buscador, com frases como "seu cartão foi bloqueado", "seus pontos vão expirar" ou "atualize seus dados". A página pede agência, conta, senha, código do token e às vezes uma foto do rosto, que o golpista usa para tentar cadastrar o aparelho dele na sua conta.

COMO SE PROTEGER

- Entre no banco só pelo aplicativo oficial ou digitando o endereço você mesmo.
- Não toque em link de mensagem que fala da sua conta, mesmo que pareça do banco.
- Banco não pede senha, código do token nem foto do rosto por link.
- Ative no aplicativo do banco os avisos de novo aparelho e de cada transação.

O QUE FAZER

1. Entre no aplicativo oficial e troque a senha. Se não conseguir entrar, ligue para o banco e peça o bloqueio.
2. Peça ao banco para descadastrar os aparelhos que você não reconhece.
3. Se apareceu Pix que você não fez, peça o MED.
4. Salve o print da mensagem e do endereço do site falso e registre o boletim de ocorrência.

4

Celular roubado ou usado por outra pessoa desbloqueado.

Quem tem a senha de bloqueio consegue abrir o banco, trocar senhas, pedir empréstimo e transferir. Por isso ladrões tentam ver a senha antes de levar o aparelho.

O QUE É

Aqui não há vírus: quem está com o celular desbloqueado, ou sabe a senha de bloqueio, usa os aplicativos como se fosse o dono.

COMO ACONTECE

O ladrão observa a pessoa digitando a senha em lugar público, ou pega o celular já desbloqueado da mão dela. Com a senha de bloqueio, ele recebe os códigos por SMS,

entra no e-mail, troca senhas e, em muitos bancos, abre o aplicativo e faz Pix. Também acontece com gente próxima que pega o celular emprestado.

COMO SE PROTEGER

- Use senha de bloqueio diferente da senha do banco e esconda a digitação.
- Ative senha ou biometria própria no aplicativo do banco, quando ele oferecer.
- Deixe o limite do Pix baixo e o limite noturno menor ainda.
- Cadastre o celular no Celular Seguro, serviço do governo federal que precisa de conta gov.br e de cadastro feito antes do roubo. Nele dá para indicar pessoas de confiança, que também podem dar o alerta.

O QUE FAZER

1. De outro telefone, ligue para o banco e peça o bloqueio da conta e do aplicativo naquele aparelho.
2. Ligue para a operadora e bloqueie o chip.
3. Use o Encontre Meu Dispositivo, do Google, para bloquear ou apagar o celular a distância.
4. Registre o boletim de ocorrência com o número IMEI do aparelho, que fica na caixa ou na nota fiscal.
5. Se cadastrou o celular no Celular Seguro, dê o alerta, você ou uma pessoa de confiança. O modo recuperação bloqueia a linha e as contas nos bancos parceiros e mantém o IMEI ativo, para ajudar a polícia a achar o aparelho; o modo bloqueio total bloqueia também o IMEI.

5 Clonagem do chip, o SIM swap.

O golpista transfere o número da vítima para um chip dele e passa a receber os códigos por SMS e as chamadas de confirmação.

O QUE É

É a transferência do seu número de telefone para um chip que está com o golpista. A partir daí, as ligações e os SMS do seu número vão para ele, inclusive os códigos de confirmação do banco e do WhatsApp.

COMO ACONTECE

O golpista usa dados vazados, como nome, CPF e data de nascimento, para pedir à operadora a troca de chip ou a portabilidade. O sinal para a vítima é claro: o celular fica sem serviço de repente e pede o chip.

COMO SE PROTEGER

- Peça à operadora uma senha para troca de chip e portabilidade.

- Ative o PIN do chip no celular, em Configurações, Segurança, Bloqueio do cartão SIM. O nome do menu muda conforme a marca.
- Onde der, use confirmação em duas etapas por aplicativo ou pelo e-mail, e não só por SMS.
- Não publique data de nascimento, CPF e outros dados pessoais em redes sociais.

O QUE FAZER

1. Se o celular ficou sem sinal sem motivo, ligue logo para a operadora, de outro telefone, e peça o bloqueio da linha e a volta do número.
2. Avise o banco e peça o bloqueio de transações enquanto o número não volta.
3. Troque as senhas do e-mail e do WhatsApp assim que recuperar o número.
4. Registre o boletim de ocorrência e, se a operadora demorar, uma reclamação na Anatel.

PARTE 2



Sinais de que a conta está em risco

1

Ligação ou mensagem "do banco" pedindo para instalar aplicativo, informar código ou fazer um Pix "de teste" ou "de segurança".

O QUE É

É o sinal mais claro de golpe em andamento. Nenhum banco pede para instalar aplicativo, repassar código recebido por SMS ou fazer um Pix "de teste" ou "de segurança" para proteger a conta.

COMO ACONTECE

O golpista assusta primeiro ("sua conta está sendo invadida agora") e oferece a solução em seguida. O "Pix de segurança" vai para uma conta dele; o código libera o seu WhatsApp ou um aparelho novo no banco; o aplicativo é o acesso remoto.

COMO SE PROTEGER

- Combine com a família: banco que pede isso é golpe, sem exceção.
- Não continue a conversa: desligue e ligue para o número oficial.
- Nunca leia em voz alta nem digite código que chegou por SMS a pedido de outra pessoa.

O QUE FAZER

1. Se instalou algum aplicativo, desligue a internet do celular.
2. Se passou código ou senha, troque as senhas a partir de outro aparelho.

3. Se fez o Pix, ligue para o banco e peça o MED na hora.

2

Aplicativo recém-instalado que pediu

Acessibilidade ou Administrador do dispositivo.

O QUE É

A Acessibilidade foi criada para ajudar pessoas com deficiência a usar o celular: ela lê a tela e toca por você. O Administrador do dispositivo dá poder para bloquear o aparelho e impedir a desinstalação. Um aplicativo comum quase nunca precisa de nenhuma das duas.

COMO ACONTECE

O trojan bancário insiste no pedido: mostra a tela de permissão várias vezes e às vezes trava o celular até a pessoa aceitar. Nas versões mais novas do Android, aplicativos instalados fora da loja aparecem com a Acessibilidade bloqueada como "configuração restrita", e o golpe ensina a liberar.

COMO SE PROTEGER

- Antes de aceitar, pergunte: esse aplicativo precisa ler a minha tela?
- Revise de tempos em tempos Configurações, Acessibilidade e Configurações, Segurança, Apps de administração do dispositivo.
- Se o Android disser que a configuração é restrita, não libere.

O QUE FAZER

1. Desligue a internet do celular.
2. Se conseguir, desative o aplicativo na Acessibilidade e no Administrador do dispositivo.
3. De outro aparelho, avise o banco e troque as senhas.
4. Formate o celular, como explica a Parte 4.

3

Tela que escurece sozinha, aviso de "atualização" que não sai, ou celular mexendo sozinho.

O QUE É

São sinais de que alguém está usando o celular a distância naquele momento.

COMO ACONTECE

O trojan escurece a tela ou põe por cima um aviso falso, como "atualizando o sistema, não desligue", enquanto abre o banco por trás. No acesso remoto, a vítima pode ver a

tela rolando, aplicativos abrindo e textos sendo digitados.

COMO SE PROTEGER

- Desconfie de "atualização" que trava a tela e não vem do próprio Android nem da Play Store.
- A atualização do sistema fica em Configurações, Sistema, Atualização de software, e não aparece de repente por cima do banco.

O QUE FAZER

1. Desligue a internet na hora, pelo painel de atalhos, ou desligue o celular segurando o botão de ligar.
2. De outro telefone, ligue para o banco e peça o bloqueio imediato.
3. Não volte a usar o banco nesse celular antes de formatar.

4

Aviso de acesso à conta em aparelho novo que você não reconhece.

O QUE É

Muitos bancos avisam por notificação, SMS ou e-mail quando a conta é acessada ou cadastrada em um aparelho novo. Se você não trocou de celular, alguém está entrando com os seus dados.

COMO ACONTECE

Depois de conseguir senha e código por site falso, por ligação ou pelo trojan, o golpista cadastra o aparelho dele como confiável, para fazer transações sem depender do seu celular.

COMO SE PROTEGER

- Ative todos os avisos de segurança no aplicativo do banco.
- No aplicativo do banco, procure a opção de aparelhos cadastrados, algo como "dispositivos" ou "aparelhos autorizados". O nome muda de um banco para outro.
- Não ignore o aviso achando que é engano.

O QUE FAZER

1. Ligue para o banco pelo número oficial, peça para descadastrar o aparelho desconhecido e bloquear a conta.
2. Troque a senha do banco e a do e-mail.
3. Confira o extrato e peça o MED para todo Pix que você não fez.

5**O celular ficou sem sinal de repente, sem motivo, e voltou a pedir o chip. Pode ser clonagem.****O QUE É**

Quando o número é transferido para outro chip, o seu para de funcionar. Por isso o celular mostra "sem serviço" ou pede o chip, mesmo onde sempre teve sinal.

COMO ACONTECE

O golpista faz a troca de chip ou a portabilidade e, logo depois, pede os códigos por SMS para entrar no WhatsApp, no e-mail e no banco. Tudo costuma acontecer em poucas horas, muitas vezes à noite ou no fim de semana.

COMO SE PROTEGER

- Peça à operadora uma senha para troca de chip e portabilidade.
- Ative o PIN do chip.
- Use confirmação em duas etapas que não dependa só do SMS.

O QUE FAZER

1. Reinicie o celular uma vez. Se continuar sem sinal, ligue para a operadora de outro telefone e pergunte se houve troca de chip.
2. Se houve, peça o bloqueio e a volta da linha, e avise o banco.
3. Troque as senhas do e-mail e do WhatsApp assim que o número voltar.

6**Pix, empréstimo ou alteração de limite que você não fez.****O QUE É**

É quando a pessoa abre o extrato e pensa: "apareceu um Pix que eu não fiz". Vale também para empréstimo contratado, cartão novo ou limite aumentado sem pedido. É sinal de que a conta já foi acessada.

COMO ACONTECE

O golpista costuma primeiro aumentar o limite do Pix ou contratar um empréstimo pré-aprovado, para ter mais dinheiro, e depois transferir tudo em vários Pix para contas diferentes, as chamadas contas laranja.

COMO SE PROTEGER

- Ative o aviso de cada transação.
- Mantenha os limites baixos e o limite noturno menor ainda.
- Confira o extrato com frequência, e não só quando chega a fatura.

O QUE FAZER

1. Ligue para o banco imediatamente e peça o bloqueio da conta e de novos empréstimos.
2. Peça o MED para cada Pix, um por um.
3. Conte o empréstimo e o aumento de limite que você não pediu.
4. Registre o boletim de ocorrência e guarde os prints do extrato.

PARTE 3



Como evitar

1 Instale aplicativos só pela Play Store.

Banco nenhum manda atualização por link.

O QUE É

A Play Store confere os aplicativos antes de publicar e tira do ar os que são descobertos como maliciosos. Fora dela, ninguém confere nada.

COMO ACONTECE

O golpe por link manda o arquivo direto justamente para fugir dessa conferência. Atualização de banco de verdade chega pela Play Store, nunca por mensagem.

COMO SE PROTEGER

- Procure o aplicativo do banco na Play Store e confira o nome do desenvolvedor.
- Desconfie de aplicativo com poucas avaliações e nome parecido com o do banco.
- Deixe desligada a permissão de instalar apps desconhecidos para o navegador, o WhatsApp e o gerenciador de arquivos.

O QUE FAZER

1. Se instalou algo por link, desligue a internet.
2. De outro aparelho, avise o banco e troque as senhas.
3. Formate o celular, como explica a Parte 4.

2 Desligue e ligue você mesmo.

Se alguém ligar dizendo ser do banco, desligue e ligue para o número que está atrás do cartão ou no aplicativo. O banco nunca pede senha, código, instalação de aplicativo nem Pix para "proteger" a conta.

O QUE É

É a regra de ouro contra a falsa central do banco: quem decide para onde ligar é você.

COMO ACONTECE

O golpista conta com o medo e a pressa para a pessoa continuar na mesma ligação. Quando você liga para o número oficial, a conversa falsa acaba ali.

COMO SE PROTEGER

- Anote o número oficial do seu banco, que está atrás do cartão e no aplicativo.
- Se der, ligue de outro telefone.
- Explique a regra para pais e avós, que são alvo frequente.

O QUE FAZER

1. Se já seguiu as instruções de um falso atendente, siga a Parte 4 deste guia desde o primeiro passo.

3 Revise a Acessibilidade.

Em Configurações, Acessibilidade, veja quais aplicativos estão ativados. Se tiver algum que você não reconhece, desative e desinstale.

O QUE É

A lista da Acessibilidade mostra quais aplicativos têm permissão para ler a tela e tocar por você.

COMO ACONTECE

O trojan bancário se esconde com nomes genéricos, como "Serviço do sistema", "Atualização" ou o nome de um banco, muitas vezes com ícone em branco.

COMO SE PROTEGER

- Abra Configurações, Acessibilidade, e veja a parte de aplicativos instalados ou baixados.
- Deixe ativado só o que você reconhece, como um leitor de tela que você mesmo instalou.
- Repita a revisão sempre que instalar um aplicativo novo.

O QUE FAZER

1. Desative o aplicativo estranho e tente desinstalar.
2. Se ele voltar a se ativar ou não deixar desinstalar, o celular precisa ser formatado.
3. De outro aparelho, avise o banco e troque as senhas.

4**Deixe o Google Play Protect ligado,**

em Play Store, perfil, Play Protect.

O QUE É

O Google Play Protect é a verificação de segurança do Android: confere os aplicativos instalados, inclusive os que vieram de fora da loja, e avisa ou desativa os perigosos.

COMO ACONTECE

Alguns golpes pedem para desligar o Play Protect, dizendo que ele "atrapalha a instalação". Esse pedido já é sinal de golpe.

COMO SE PROTEGER

- Abra a Play Store, toque na foto do perfil, em Play Protect, e deixe a verificação ligada.
- Toque em Verificar de vez em quando.
- Nunca desligue o Play Protect porque alguém pediu.

O QUE FAZER

1. Se o Play Protect avisou sobre um aplicativo, desinstale e avise o banco.
2. Se a conta já foi acessada, formate o celular.

5**Use senha de bloqueio forte**

e diferente da senha do banco. Evite data de nascimento e sequências. Esconda a digitação em lugares públicos.

O QUE É

A senha de bloqueio é a porta de entrada de tudo o que está no celular, inclusive do banco.

COMO ACONTECE

Ladrões observam a digitação no ônibus, na fila e no bar antes de levar o aparelho. Senhas como 123456, a data de nascimento ou o desenho em L são descobertas em segundos.

COMO SE PROTEGER

- Use senha com 6 dígitos ou mais, sem sequência e sem data, ou uma senha com letras e números.
- Não use a mesma senha no banco.
- Em lugar público, desbloqueie com a biometria para não precisar digitar a senha.

O QUE FAZER

1. Se alguém viu a sua senha, troque agora.
2. Se o celular foi roubado, siga o item 4 da Parte 1.

6 Ajuste os limites do Pix

no aplicativo do banco. Deixe o limite noturno baixo e o limite diário compatível com o seu uso. Aumentar limite costuma levar um tempo de espera, o que atrapalha o golpista.

O QUE É

O limite do Pix é o valor máximo que pode sair da conta por transação, por dia e no período noturno. Limite baixo não impede o golpe, mas diminui o prejuízo.

COMO ACONTECE

Pela regra do Banco Central, o período noturno vai das 20h às 6h, e o pedido para aumentar o limite só passa a valer depois de um prazo de 24 a 48 horas; para diminuir, vale na hora. Esse tempo de espera dá chance de perceber o golpe e bloquear.

COMO SE PROTEGER

- No aplicativo do banco, procure a opção de limites do Pix e ajuste. O nome muda de um banco para outro.
- Deixe o limite noturno bem baixo.
- Se precisar de um valor maior uma vez, aumente com antecedência e depois volte ao normal.

O QUE FAZER

1. Se ainda tiver acesso ao aplicativo, reduza os limites na hora.
2. Ligue para o banco e peça o bloqueio do Pix.

7 Cadastre só os seus aparelhos

como confiáveis no banco e ative os avisos de cada transação.

O QUE É

O banco guarda a lista dos celulares autorizados a usar a conta. Pela regra do Banco Central, em vigor desde novembro de 2024, o Pix feito em aparelho não cadastrado no banco fica limitado a R\$ 200 por transação e R\$ 1.000 por dia, até o aparelho ser cadastrado no banco.

COMO ACONTECE

O golpista tenta cadastrar o aparelho dele com os seus dados e códigos. O aviso de novo aparelho é a chance de barrar isso a tempo.

COMO SE PROTEGER

- No aplicativo do banco, procure a opção de aparelhos cadastrados (o nome muda de um banco para outro), confira a lista e remova os que não são seus.
- Ative a notificação de cada Pix, compra e acesso.
- Ao trocar de celular, descadastre o antigo.

O QUE FAZER

1. Se aparecer aparelho desconhecido, ligue para o banco e peça o bloqueio da conta.

8

Peça à operadora uma senha

para troca de chip e portabilidade.

O QUE É

É uma senha combinada com a operadora, pedida antes de trocar o chip ou de levar o número para outra operadora.

COMO ACONTECE

Sem essa senha, basta o golpista ter os seus dados pessoais para tentar a troca. Com ela, o pedido fica bem mais difícil.

COMO SE PROTEGER

- Ligue para a operadora, ou use o aplicativo dela, e pergunte como cadastrar a senha de segurança.
- Ative também o PIN do chip no celular.
- Guarde a senha longe do celular.

O QUE FAZER

1. Se o número já foi transferido, siga o sinal 5 da Parte 2.

9

Mantenha o sistema e os aplicativos atualizados.

O QUE É

As atualizações do Android e dos aplicativos fecham falhas de segurança que os golpistas usam.

COMO ACONTECE

Celular desatualizado fica exposto a falhas conhecidas. E as versões mais novas do Android trazem proteções contra o golpe por link, como o bloqueio de permissões sensíveis para aplicativos de fora da loja.

COMO SE PROTEGER

- Instale as atualizações em Configurações, Sistema, Atualização de software.
- Deixe a atualização automática ligada na Play Store.
- Se o celular não recebe mais atualizações, redobre o cuidado com o banco nele.

O QUE FAZER

1. Atualizar não remove um golpe já instalado. Se a conta foi invadida, siga a Parte 4.

10

Não deixe o banco aberto em celular emprestado

e não empreste o celular desbloqueado.

O QUE É

O banco aberto, ou com a senha salva, no celular de outra pessoa é uma porta aberta para quem está com o aparelho.

COMO ACONTECE

A pessoa entra no banco pelo celular de um parente, de um colega ou de uma loja e esquece de sair. Ou empresta o próprio celular desbloqueado, e alguém usa o banco sem ela ver.

COMO SE PROTEGER

- Não entre no banco em celular que não é seu.
- Se precisar entrar, saia da conta no fim e apague os dados do aplicativo.
- Ao emprestar o celular, use o modo convidado ou fixe a tela em um aplicativo, quando o seu Android oferecer.

O QUE FAZER

1. Se usou o banco em outro aparelho, troque a senha e peça ao banco para descadastrar esse aparelho.

PARTE 4



Se a conta já foi invadida

Nas primeiras horas

1

Ligue para o banco imediatamente,

pelo número oficial, de outro telefone se possível. Peça o bloqueio da conta, do cartão, do Pix e de novos empréstimos.

O QUE É

É o primeiro passo e o mais urgente. O bloqueio impede novos Pix, empréstimos e compras enquanto você resolve o resto.

COMO ACONTECE

O golpista age rápido: costuma tirar o dinheiro em poucos minutos e espalhar por várias contas. Cada minuto conta.

COMO SE PROTEGER

- Ligue para o número atrás do cartão ou do site oficial do banco, nunca para um número recebido por mensagem.
- Use outro telefone, porque o celular infectado pode estar sendo controlado.
- Anote o número do protocolo do atendimento.

O QUE FAZER

1. Peça o bloqueio da conta, do cartão, do Pix e de novos empréstimos.
2. Peça para descadastrar os aparelhos que você não reconhece.
3. Pergunte como acompanhar a contestação e anote o protocolo.

2

Peça a devolução pelo Mecanismo Especial de Devolução, o MED,

para cada Pix feito sem você. O prazo é de até 80 dias depois do Pix, mas quanto antes, maior a chance de o dinheiro ainda estar na conta do golpista. O pedido também pode ser feito pela área do Pix no aplicativo do banco, na opção de contestar.

O QUE É

O Mecanismo Especial de Devolução, o MED, é a regra do Banco Central que permite bloquear e devolver o dinheiro de um Pix feito em golpe, se ele ainda estiver na conta

de quem recebeu.

COMO ACONTECE

Você pede ao seu banco, que avisa o banco de quem recebeu. Esse banco bloqueia o valor que encontrar na conta, analisa o pedido em até 7 dias e, se confirmar o golpe, devolve o valor que ainda estiver bloqueado na conta do golpista. A vítima pode pedir o MED até 80 dias depois do Pix.

A versão nova do MED segue o dinheiro por até 5 transferências seguidas em contas de repasse, as contas laranja, para bloquear os valores em vários bancos ao mesmo tempo.

COMO SE PROTEGER

- Peça o MED o quanto antes: o golpista tira o dinheiro rápido.
- Peça um para cada Pix, com data, hora, valor e nome de quem recebeu.
- Se o seu banco tiver, procure no aplicativo, na parte do Pix, algo como "contestar" ou "devolução". O nome muda de um banco para outro, e a opção funciona a qualquer hora.

O QUE FAZER

1. Ligue para o banco ou abra a contestação pelo aplicativo, na parte do Pix.
2. Guarde o protocolo de cada pedido.
3. Acompanhe a resposta. Se o banco não resolver, registre reclamação no Banco Central e no consumidor.gov.br.

3

Registre um boletim de ocorrência,

que pode ser feito pela delegacia eletrônica do seu estado. Ele ajuda na contestação com o banco.

O QUE É

O boletim de ocorrência é o registro oficial do crime na polícia.

COMO ACONTECE

Na maioria dos estados, o golpe pela internet pode ser registrado na delegacia eletrônica, no site da Polícia Civil, sem sair de casa.

COMO SE PROTEGER

- Conte o que aconteceu na ordem: a ligação ou a mensagem, o aplicativo instalado, os Pix e os valores.
- Informe os números de telefone, os nomes e as chaves Pix usados pelo golpista.
- Guarde o número do boletim.

O QUE FAZER

1. Envie o boletim ao banco junto com a contestação.
2. Use o mesmo boletim nas reclamações em outros órgãos, se precisar.

4

Guarde as provas:

prints dos Pix, das conversas, do número que ligou e dos aplicativos instalados.

O QUE É

As provas mostram ao banco e à polícia o que aconteceu e ajudam na contestação.

COMO ACONTECE

Muitas provas somem rápido: o golpista apaga conversas, o aplicativo some e a formatação do celular apaga o resto.

COMO SE PROTEGER

- Faça prints dos comprovantes dos Pix, do extrato, das conversas, do número que ligou e da lista de aplicativos instalados.
- Copie os prints para outro aparelho ou para o e-mail antes de formatar.
- Anote a data e a hora de cada fato.

O QUE FAZER

1. Junte as provas numa pasta e envie ao banco e à polícia as que forem pedidas.



Depois, no celular: formatar é obrigatório

Se a conta foi invadida pelo celular, o aparelho precisa ser formatado, ou seja, voltar às configurações de fábrica. Apagar só o aplicativo suspeito não basta: o golpista pode ter deixado outro aplicativo escondido, uma permissão ativa ou um acesso remoto que continua funcionando. Enquanto o celular não for formatado, qualquer senha nova digitada nele pode ser roubada de novo.

1

Não use esse celular para o banco, o e-mail ou o WhatsApp

até ele ser formatado.

O QUE É

Enquanto o golpe estiver no aparelho, tudo o que você digita nele pode ser visto pelo golpista.

COMO ACONTECE

O trojan e o acesso remoto continuam funcionando mesmo depois de a conta ser bloqueada, esperando a próxima senha.

COMO SE PROTEGER

- Use outro celular ou um computador de confiança para o banco, o e-mail e o WhatsApp.
- Não digite senha nova nesse aparelho.

O QUE FAZER

1. Se digitou senha nova nele, troque de novo a partir de outro aparelho.

2 Desligue a internet

do aparelho, tirando o Wi-Fi e os dados móveis, para cortar o acesso do golpista.

O QUE É

Sem internet, o golpista perde o controle do aparelho e não recebe mais o que o golpe captura.

COMO ACONTECE

O acesso remoto e o trojan dependem da internet para receber ordens e mandar os dados.

COMO SE PROTEGER

- Desligue o Wi-Fi e os dados móveis no painel de atalhos, ou ative o modo avião.
- Mantenha desligado até a hora de formatar.

O QUE FAZER

1. Se a internet voltar a ligar sozinha, desligue o celular até a hora de formatar.

3 Tire os prints das provas antes,

porque a formatação apaga tudo.

O QUE É

A formatação apaga tudo o que está no celular, inclusive as provas do golpe.

COMO ACONTECE

Depois de formatado, não dá para recuperar a conversa com o golpista nem o nome do aplicativo instalado.

COMO SE PROTEGER

- Faça os prints com a internet desligada.
- Copie os prints para um computador pelo cabo, ou fotografe a tela com outro celular.

O QUE FAZER

1. Se já formatou sem os prints, use o extrato do banco e o histórico de ligações da operadora como prova.

4

Troque as senhas

do banco, do e-mail principal e do WhatsApp a partir de outro aparelho, e ative a confirmação em duas etapas.

O QUE É

As senhas antigas podem estar com o golpista. Trocar a partir de outro aparelho garante que ele não veja as novas.

COMO ACONTECE

Com o e-mail principal, o golpista recupera a senha de quase todas as outras contas. Por isso o e-mail é tão importante quanto o banco.

COMO SE PROTEGER

- Troque primeiro a senha do e-mail principal, depois a do banco e a do WhatsApp.
- Ative a confirmação em duas etapas no e-mail, no WhatsApp e no banco.
- Use uma senha diferente em cada serviço.

O QUE FAZER

1. Se não consegue entrar no e-mail, use a recuperação de conta do Google em outro aparelho.

5

Salve só fotos, vídeos e contatos,

de preferência copiando para um computador. Não salve nem restaure o backup dos aplicativos, porque ele pode trazer o golpe de volta.

O QUE É

Fotos, vídeos e contatos são arquivos comuns e não levam o golpe junto. Já o backup dos aplicativos e das configurações pode trazer de volta o aplicativo malicioso ou a permissão que ele recebeu.

COMO ACONTECE

Ao restaurar um backup completo, o Android reinstala os aplicativos da lista e pode recuperar os dados e as configurações deles.

COMO SE PROTEGER

- Copie fotos e vídeos para um computador pelo cabo.
- Confira se os contatos estão salvos na conta do Google.
- Ao configurar o celular formatado, não restaure o backup: escolha configurar como novo.

O QUE FAZER

1. Se restaurou o backup e algo estranho voltou, formate de novo sem restaurar nada.

6

Formate o celular

em Configurações, Sistema, Redefinir, Restaurar configuração original. O nome do menu muda um pouco de uma marca para outra. Se o celular não deixar, desligue, segure Volume para baixo e o botão de ligar até abrir o modo de recuperação e escolha "Wipe data / factory reset". Se nem isso funcionar, leve a uma assistência técnica de confiança.

O QUE É

Formatar, ou restaurar a configuração de fábrica do Android, apaga todos os aplicativos, dados e configurações e deixa o celular como saiu da caixa.

COMO ACONTECE

O caminho mais comum é Configurações, Sistema, Redefinir, Restaurar configuração original. Na Samsung, costuma ser Configurações, Gerenciamento geral, Restaurar, Restaurar padrão de fábrica.

Se o golpe não deixar abrir as configurações, o modo de recuperação apaga tudo antes de o Android carregar. A combinação de botões muda conforme a marca.

COMO SE PROTEGER

- Anote o e-mail e a senha da sua conta Google antes de formatar. Depois da formatação o celular pede essa conta, e sem ela ele fica travado.
- Carregue a bateria acima da metade.
- Tire o cartão de memória, se houver, e não use os aplicativos guardados nele.

O QUE FAZER

1. Anote o e-mail e a senha da sua conta Google antes de formatar. Depois da formatação o celular pede essa conta, e sem ela ele fica travado.

2. Abra Configurações, Sistema, Redefinir, e escolha Restaurar configuração original, ou Apagar todos os dados.
3. Confirme com a senha de bloqueio e espere o celular reiniciar.
4. Se não der: desligue, segure Volume para baixo e o botão de ligar, escolha "Wipe data / factory reset" com os botões de volume e confirme com o botão de ligar.
5. Se nada disso funcionar, leve a uma assistência técnica de confiança.

7 Depois de formatar, instale os aplicativos de novo só pela Play Store,

um por um, e entre no banco só depois de conferir que nenhum aplicativo estranho voltou e que a Acessibilidade está limpa.

O QUE É

Depois de formatado, o celular está limpo. O cuidado agora é não trazer o golpe de volta.

COMO ACONTECE

O golpe volta quando a pessoa restaura o backup ou instala de novo o mesmo aplicativo por link.

COMO SE PROTEGER

- Instale os aplicativos pela Play Store, um por um, só os que você usa.
- Antes de entrar no banco, confira a lista de aplicativos e a Acessibilidade.
- Depois de entrar, confira os aparelhos cadastrados no banco.

O QUE FAZER

1. Se aparecer de novo um aplicativo que você não instalou, desligue a internet e procure uma assistência técnica.

8 Se o celular ficou sem sinal,

ligue para a operadora e confirme se o chip foi trocado sem você.

O QUE É

Se o celular ficou sem sinal durante o golpe, o número pode ter sido levado para outro chip.

COMO ACONTECE

Com o número, o golpista recebe os códigos por SMS e entra de novo nas contas, mesmo com o celular já formatado.

COMO SE PROTEGER

- Ligue para a operadora e pergunte se houve troca de chip ou portabilidade.
- Cadastre a senha de segurança para troca de chip.

O QUE FAZER

1. Se houve troca, peça o bloqueio e a volta da linha, e anote o protocolo.

9**Confira o Registrato do Banco Central**

para ver se abriram conta ou pegaram empréstimo no seu nome.

O QUE É

O Registrato é um serviço gratuito do Banco Central que mostra as contas, os empréstimos e as chaves Pix ligados ao seu CPF em todos os bancos.

COMO ACONTECE

Com os seus dados, o golpista pode abrir conta ou pegar empréstimo em outro banco, no seu nome, sem você saber.

COMO SE PROTEGER

- Entre no Registrato pelo site do Banco Central, com a conta gov.br.
- Confira os relatórios de contas, de empréstimos e de chaves Pix.
- Repita a consulta alguns meses depois.

O QUE FAZER

1. Se aparecer conta ou empréstimo que você não fez, procure o banco que aparece no relatório e registre o boletim de ocorrência.

MENSAGEM PRONTA PARA AVISAR SEUS CONTATOS

Pessoal, tiveram acesso à minha conta do banco pelo celular. Se alguém ligar dizendo ser do banco e pedir para instalar aplicativo, informar código ou fazer Pix, desliguem e liguem vocês mesmos para o número oficial. E nunca instalem aplicativo de banco por link.

DÚVIDAS COMUNS

Perguntas frequentes

❓ Como invadiram minha conta pelo celular?

Na maioria dos casos o banco não foi invadido: o golpista entrou pelo celular da vítima, ou convenceu a vítima a abrir a porta para ele. Os caminhos mais usados no Android são o aplicativo malicioso instalado por link, que recebe a permissão de Acessibilidade e faz Pix sozinho; a falsa central do banco, que pede para instalar um aplicativo de acesso remoto (o golpe da mão fantasma); o site ou a mensagem falsa do banco; o celular roubado ou usado desbloqueado por outra pessoa; e a clonagem do chip.

❓ O banco liga pedindo para instalar aplicativo?

Não. O banco nunca pede senha, código, instalação de aplicativo nem Pix para "proteger" a conta. Se alguém ligar dizendo ser do banco, desligue e ligue você mesmo para o número que está atrás do cartão ou no aplicativo.

❓ Como pedir o MED do Pix?

Ligue para o banco pelo número oficial e peça a devolução pelo Mecanismo Especial de Devolução, o MED, para cada Pix feito sem você. O pedido também pode ser feito pela área do Pix no aplicativo do banco, na opção de contestar. O prazo é de até 80 dias depois do Pix, mas quanto antes, maior a chance de o dinheiro ainda estar na conta do golpista. O banco analisa o pedido em até 7 dias e, se confirmar o golpe, devolve o valor que ainda estiver bloqueado na conta do golpista.

❓ Preciso formatar o celular depois do golpe?

Sim. Se a conta foi invadida pelo celular, o aparelho precisa ser formatado, ou seja, voltar às configurações de fábrica. Enquanto o celular não for formatado, qualquer senha nova digitada nele pode ser roubada de novo.

? Apagar só o aplicativo resolve?

Não basta. O golpista pode ter deixado outro aplicativo escondido, uma permissão ativa ou um acesso remoto que continua funcionando. Por isso o celular precisa ser formatado.

? Posso restaurar o backup depois de formatar?

Salve só fotos, vídeos e contatos, de preferência copiando para um computador. Não salve nem restaure o backup dos aplicativos, porque ele pode trazer o golpe de volta. Depois de formatar, instale os aplicativos de novo só pela Play Store, um por um.

Precisa de ajuda?

A JAL Softwares, por meio da Vortex CyberSegurança, ajuda a identificar como o celular foi invadido, a limpar o aparelho e a proteger as contas. Fale com a gente pelo WhatsApp (17) 99197-2287, pelo e-mail contato@sistemasvortex.com.br ou pelo site sistemasvortex.com.br.

✉ contato@sistemasvortex.com.br

📷 [@jalsoftwares](https://www.instagram.com/jalsoftwares)

 Chamar no WhatsApp

Última atualização: 20 de outubro de 2026.