

DICAS DE SEGURANÇA

Celular hackeado: como identificar, prevenir e resolver no Android e no iPhone

Um celular invadido não é só um aparelho lento. É acesso ao seu banco, ao seu WhatsApp, às suas fotos e aos seus contatos. Este guia mostra os sinais de que algo está errado, como se proteger e o que fazer se já aconteceu, no Android e no iPhone.

Guia da JAL Softwares e da Vortex CyberSegurança. Atualizado em 18/10/2026.



PARTE 1

Sinais de que o celular foi invadido

Fique atento se o celular apresentar dois ou mais destes sinais ao mesmo tempo:

- 1** Bateria acabando em poucas horas, mesmo sem uso.
- 2** Aparelho quente e lento o tempo todo, travando em tarefas simples.
- 3** Consumo de internet muito acima do normal.
- 4** Aplicativos que você não instalou, ou ícones que somem e aparecem.
- 5** Anúncios e janelas abrindo sozinhos, mesmo fora do navegador.
- 6** Tela acendendo, apps abrindo ou mensagens sendo enviadas sem você fazer nada.
- 7** Contatos recebendo mensagens que você não mandou.
- 8** Avisos de login em lugares desconhecidos no e-mail, no banco ou nas redes.

- 9 Configurações alteradas sozinhas: novo administrador do dispositivo, serviço de acessibilidade ligado, perfil de configuração instalado.

- 10 No extremo, o celular travado numa tela de bloqueio estranha ou sem conseguir ligar.



Um sinal isolado pode ser só um problema do aparelho. Vários juntos pedem ação imediata.



PARTE 2

Como o golpe acontece



No Android

ANDROID

O caminho mais comum é um aplicativo malicioso instalado fora da Play Store, o chamado APK. Ele chega por link no WhatsApp, SMS ou e-mail, disfarçado de:

- atualização do aplicativo do banco;
- rastreio de encomenda ou liberação de taxa;
- benefício do governo, prêmio ou desconto;
- vídeo exclusivo, jogo ou aplicativo "premium" de graça.

Depois de instalado, ele pede permissão de Acessibilidade ou de Administrador do dispositivo. Com isso, consegue ler a tela, digitar por você, roubar senhas de banco e impedir a própria desinstalação. Os tipos mais comuns são:

- Trojan bancário: rouba senhas e faz transferências. É o mais frequente no Brasil.



No iPhone

IPHONE

No iPhone, aplicativo malicioso é raro, porque só instala pela App Store. O golpe muda de forma:

- Roubo da conta Apple, o Apple ID: o golpista consegue a senha por um e-mail ou SMS falso de "conta bloqueada", ou vê a senha de bloqueio por cima do ombro e rouba o aparelho. Com a senha de bloqueio, ele troca a senha do Apple ID e toma o iPhone, o iCloud e as fotos.
- Bloqueio de Ativação: ativado a partir de outra conta, deixa o aparelho inutilizável mesmo depois de restaurar.
- Perfil de configuração ou gerenciamento instalado por link: aplicativo "gratuito" fora da loja que passa a controlar o aparelho.
- Espionagem por compartilhamento: localização, Buscar ou backup sincronizado no aparelho de outra pessoa.

- Spyware ou stalkerware: espiona mensagens, chamadas e localização. Muitas vezes é instalado por alguém próximo, com o celular na mão.
- Trojan de acesso remoto: entrega o controle total do aparelho ao golpista.
- Bloqueador de tela: trava o celular e pede dinheiro para liberar.

- Jailbreak: remove as proteções do sistema e abre a porta para tudo acima.



PARTE 3

Como prevenir

Vale para os dois

- 1 Nunca instale aplicativo por link. Só pela Play Store ou pela App Store.
- 2 Desconfie de toda mensagem com urgência: "atualize agora", "sua conta será bloqueada", "última chance".
- 3 Mantenha o sistema e os aplicativos atualizados.
- 4 Use senha de bloqueio longa, com letras e números, e proteja a digitação em público.
- 5 Ative a autenticação de dois fatores no e-mail, no banco, no WhatsApp e nas redes sociais.
- 6 Não empreste o celular desbloqueado. Espionagem por gente próxima começa assim.
- 7 Faça backup das fotos e contatos em lugar seguro, para poder apagar o celular sem medo.

Só no Android

ANDROID

- 8 Deixe o Google Play Protect ligado, em Play Store, perfil, Play Protect.
- 9 Não dê permissão de Acessibilidade nem de Administrador do dispositivo para aplicativo que não precisa disso.

Só no iPhone

IPHONE

- 11 Ative a Proteção de Dispositivo Roubado, em Ajustes, Face ID e Código.
- 12 Nunca instale perfil de configuração. Confira em Ajustes, Geral, VPN e Gerenciamento de Dispositivo.

10

Confira de tempos em tempos a lista de aplicativos instalados e remova o que não reconhece.

13

Não faça jailbreak.

14

Guarde a nota fiscal. É ela que recupera o aparelho na Apple se houver bloqueio.



PARTE 4

Se o golpe já aconteceu

Primeiro, de outro aparelho

1

Troque as senhas do e-mail principal, do banco e das redes sociais.

2

Avise o banco e peça para bloquear transações.

3

Confira se não houve Pix, empréstimo ou compra feita sem você.

4

Avise seus contatos com a mensagem pronta no fim deste guia.



No Android

ANDROID

1

Reinicie em modo seguro: segure o botão de desligar, depois segure "Desligar" na tela até aparecer "Reiniciar em modo seguro". Nesse modo os aplicativos instalados não rodam.

2

Vá em Configurações, Apps, e desinstale tudo que não reconhece, começando pelos mais recentes.

3

Se não deixar desinstalar: em Configurações, Segurança, Apps de administração do dispositivo, desmarque o aplicativo. Em Acessibilidade, desative serviços estranhos. Depois desinstale.



No iPhone

IPHONE

1

Em Ajustes, toque no seu nome e veja a lista de dispositivos. Remova os que não reconhece.

2

Troque a senha do Apple ID e ative os dois fatores.

3

Em Ajustes, Geral, VPN e Gerenciamento de Dispositivo, remova perfis que você não instalou.

4

Em Ajustes, Privacidade e Segurança, use a Verificação de Segurança. Ela mostra tudo que está sendo compartilhado e com quem, e permite cortar tudo de uma vez.

5

Se precisar, restaure em Ajustes, Geral, Transferir ou Redefinir o iPhone, e não restaure um backup suspeito.

4

Se o problema continuar, faça a redefinição de fábrica em Configurações, Sistema, Redefinir. Salve antes só fotos e contatos, nunca os aplicativos.

5

Se o celular não liga nem em modo seguro: 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 abrir, é preciso reinstalar o sistema pelo computador com a ferramenta do fabricante, um serviço de assistência técnica.

6

Se o aparelho estiver travado por Bloqueio de Ativação de outra conta, só a Apple resolve, com a nota fiscal em mãos.

Depois de limpar

- Reative os dois fatores em todas as contas.
- Troque de novo as senhas que foram usadas no aparelho infectado.
- Registre boletim de ocorrência se houve prejuízo. Pode ser feito online na delegacia eletrônica do seu estado.

MENSAGEM PRONTA PARA AVISAR SEUS CONTATOS

Oi, aqui é [SEU NOME]. Meu celular foi invadido. Se você receber mensagem minha pedindo dinheiro, Pix, código ou link, não é eu. Não responda e me avise por ligação. Estou resolvendo. Obrigado.

Precisa de ajuda?

A JAL Softwares, por meio da Vortex CyberSegurança, atende casos de celular invadido, limpeza do aparelho e recuperação de contas. Fale com a gente pelo WhatsApp (17) 99197-2287 ou pelo site sistemasvortex.com.br.

[Chamar no WhatsApp](#)

Última atualização: 18 de outubro de 2026.