

DICAS DE SEGURANÇA

Black Friday sem golpe: como comprar online com segurança

A Black Friday de 2026 cai em 27 de novembro, e as semanas antes dela são as preferidas dos golpistas. Eles copiam lojas conhecidas, criam anúncios com preços impossíveis e mandam mensagens de "pedido com problema". Este guia mostra como reconhecer cada golpe, como conferir uma loja antes de pagar e o que fazer se você já caiu.

Guia da JAL Softwares e da Vortex CyberSegurança. Atualizado em 19/10/2026.

PARTE 1



Os golpes mais comuns na Black Friday

1

Loja falsa que imita uma marca conhecida.

O site copia o visual, o logo e as fotos de uma loja real, mas o endereço é diferente, com letras trocadas, palavras a mais ou terminação estranha.

O QUE É

Um site montado para parecer o de uma loja famosa: mesmo logo, mesmas cores, mesmas fotos e até os mesmos textos, copiados da loja verdadeira. A diferença está no endereço, que é parecido mas não é o oficial. O pagamento vai para o golpista e o produto nunca chega.

COMO ACONTECE

O golpista registra um endereço quase igual ao da marca, com uma letra trocada, uma palavra a mais (como "oferta", "promo" ou "blackfriday") ou outra terminação. Depois divulga o link por anúncio, mensagem ou e-mail. Esses sites costumam ficar no ar por poucos dias e mudar de endereço quando são denunciados.

COMO PREVENIR

- Digite você mesmo o endereço da loja ou use o aplicativo oficial dela.
- Antes de pagar, leia o endereço inteiro na barra do navegador, letra por letra.
- Lembre que o cadeado só mostra que a conexão é protegida; site falso também tem cadeado.
- Confira o CNPJ no rodapé e consulte na Receita Federal.
- Para endereços terminados em .br, a consulta "whois" do Registro.br mostra a data em que o endereço foi criado; site criado há poucos dias é sinal de alerta. Para outras terminações, como .com, existem consultas "whois" parecidas.

SE JÁ ACONTECEU

1. Ligue para o banco pelo número atrás do cartão ou dentro do aplicativo e peça o bloqueio do cartão e a contestação da compra.
2. Se pagou por Pix, peça ao banco a abertura do Mecanismo Especial de Devolução (MED).
3. Salve prints do site, do endereço completo na barra do navegador, do pedido e do comprovante.
4. Registre um boletim de ocorrência na delegacia eletrônica do seu estado.
5. Avise a loja verdadeira pelos canais oficiais, para que ela peça a retirada do site falso.

2 Preço bom demais para ser verdade.

Celular, TV ou eletrodoméstico pela metade do preço de todas as outras lojas. É a isca principal.

O QUE É

Um produto caro e muito procurado (celular, TV, videogame, eletrodoméstico) anunciado pela metade do preço ou menos. O preço é a isca que faz a pessoa pagar rápido, sem conferir a loja.

COMO ACONTECE

O anúncio aparece em rede social, em site de busca ou em mensagem encaminhada, quase sempre com urgência: "só hoje", "últimas unidades", contador regressivo. O

pagamento costuma ser só por Pix ou boleto, que não podem ser contestados como o cartão.

COMO PREVENIR

- Compare o preço em outras lojas grandes. Se só uma loja tem o produto muito mais barato, desconfie.
- Acompanhe o preço dos produtos que você quer nas semanas anteriores, para saber se o desconto é real.
- Não decida com pressa por causa de contador ou de "últimas unidades".
- Antes de pagar, faça as conferências da Parte 2 do guia (endereço, CNPJ, reputação e contato).

SE JÁ ACONTECEU

1. Se pagou com cartão, ligue para o banco e peça a contestação da compra.
2. Se pagou por Pix, peça ao banco a abertura do MED o quanto antes.
3. Se pagou boleto, avise o banco na hora e registre boletim de ocorrência. Em geral o boleto pago não pode ser cancelado, mas o aviso rápido ajuda o banco a tentar bloquear o valor.
4. Registre um boletim de ocorrência e guarde os prints do anúncio e do pagamento.

3

Anúncio patrocinado em rede social.

O anúncio leva para uma loja falsa. Estar patrocinado não quer dizer que a loja foi verificada.

O QUE É

Um anúncio pago, com a marcação "Patrocinado", que leva para uma loja falsa. Muita gente acha que a rede social confere quem anuncia, mas estar patrocinado só quer dizer que alguém pagou pela divulgação.

COMO ACONTECE

O golpista cria uma página com nome e foto parecidos com os de uma marca, paga pelo anúncio e escolhe quem vai ver, por idade, cidade e interesses. O link do anúncio leva para a loja falsa ou para uma conversa no WhatsApp.

COMO PREVENIR

- Não compre pelo link do anúncio. Abra o site ou o aplicativo oficial da loja e procure o produto lá.
- Toque no nome da página que anuncia e veja há quanto tempo ela existe e quantos seguidores tem.

- Na Biblioteca de Anúncios da Meta dá para ver todos os anúncios que uma página está veiculando; muitos anúncios de marcas diferentes na mesma página são sinal de golpe.

SE JÁ ACONTECEU

1. Siga os passos de banco, MED e boletim de ocorrência do golpe 1.
2. Denuncie o anúncio na própria rede social, pelo menu do anúncio (os três pontinhos), escolhendo a opção de golpe ou fraude. O nome da opção pode variar conforme a versão do aplicativo.
3. Guarde o print do anúncio com o nome da página que anunciou.

4**Perfil falso que vende pelo Instagram ou WhatsApp.**

Fotos bonitas, comentários de clientes inventados, pagamento só por Pix e o produto nunca chega.

O QUE É

Um perfil que se apresenta como loja, com fotos bonitas, muitos seguidores e comentários de clientes satisfeitos, mas que não tem empresa por trás. Os seguidores podem ser comprados e os comentários, inventados.

COMO ACONTECE

O atendimento é todo por mensagem. O vendedor manda fotos do produto, às vezes "comprovantes" de outros clientes, e pede o pagamento por Pix, muitas vezes para uma pessoa física. Depois do pagamento, some, bloqueia o cliente ou pede mais dinheiro para "liberar o envio".

COMO PREVENIR

- Desconfie de loja que só existe em rede social e não tem site, CNPJ nem endereço.
- No Instagram, toque nos três pontinhos do perfil e em "Sobre esta conta" para ver desde quando ele existe e se mudou de nome.
- Procure o nome da loja e o CNPJ em sites de reclamação.
- Prefira pagar por cartão ou por um meio com proteção ao comprador.

SE JÁ ACONTECEU

1. Siga os passos de banco, MED e boletim de ocorrência do golpe 1.
2. Salve prints do perfil (com o nome de usuário), das conversas e do comprovante antes que o perfil seja apagado.
3. Denuncie o perfil na rede social.
4. Se a conversa foi pelo WhatsApp, denuncie e bloqueie o número pelo próprio aplicativo.

5**Pagamento só por Pix, para pessoa física.**

A loja não aceita cartão nem boleto e pede Pix para uma conta no nome de uma pessoa, não da empresa.

O QUE É

A "loja" não aceita cartão nem boleto e pede um Pix para uma conta no nome de uma pessoa, e não da empresa. O Pix cai na hora e não tem contestação como a do cartão, por isso é o meio preferido do golpista.

COMO ACONTECE

O vendedor dá uma desculpa: "o sistema de cartão está fora do ar", "Pix tem desconto", "a conta é do dono da loja". Às vezes mostra um QR Code numa página que parece um checkout real.

COMO PREVENIR

- Antes de confirmar o Pix, leia o nome e o CNPJ ou CPF do recebedor que aparecem no aplicativo do banco.
- O nome tem que ser o da empresa que você conferiu. Se for o de uma pessoa ou de outra empresa, cancele.
- Desconfie de loja que não aceita cartão de crédito.

SE JÁ ACONTECEU

1. Peça ao banco a abertura do MED na hora, pelo aplicativo ou pela central. Quanto antes, maior a chance de o dinheiro ainda estar na conta do golpista.
2. O pedido do MED tem prazo de até 80 dias depois do Pix. Os bancos são obrigados a oferecer a contestação dentro da área do Pix no aplicativo.
3. O MED não garante a devolução: o banco do golpista bloqueia o que ainda houver na conta e analisa o caso.
4. Registre um boletim de ocorrência e entregue o número ao banco.

6

Mensagem falsa de entrega.

SMS, e-mail ou WhatsApp dizendo que o pedido está retido, que falta pagar uma taxa ou que o endereço está errado, com um link para "resolver".

O QUE É

Um SMS, e-mail ou WhatsApp que finge ser de transportadora, dos Correios ou da loja e diz que o pedido está retido, que falta pagar uma taxa ou que o endereço está errado. O link leva para uma página falsa que cobra a taxa ou pede os dados do cartão.

COMO ACONTECE

O golpista manda a mesma mensagem para milhares de números, sabendo que na Black Friday muita gente está esperando uma entrega. A página falsa copia o visual dos Correios ou da transportadora e pede um valor pequeno, para a pessoa não pensar muito.

COMO PREVENIR

- Não clique no link da mensagem. Acompanhe a entrega pelo site ou aplicativo da loja onde você comprou, ou pelo código de rastreio que a loja informou.

- Os Correios não cobram taxa por link enviado em SMS ou WhatsApp; a taxa de importação, quando existe, é paga no site ou aplicativo oficial dos Correios, em "Minhas Importações".
- Desconfie de qualquer taxa para "liberar" uma entrega de compra feita no Brasil.

SE JÁ ACONTECEU

1. Se pagou a taxa ou digitou o cartão, ligue para o banco, peça o bloqueio do cartão e conteste a cobrança.
2. Se pagou por Pix, peça a abertura do MED.
3. Se informou senha ou código, troque as senhas do banco e do e-mail a partir de outro aparelho.
4. Registre um boletim de ocorrência.

7 Falso cupom ou sorteio.

Mensagem prometendo cupom de desconto ou prêmio, pedindo dados pessoais ou um pagamento pequeno para liberar.

O QUE É

Uma mensagem que promete cupom de desconto, vale-compras ou prêmio de uma loja conhecida, mas pede dados pessoais, dados do cartão ou um pagamento pequeno para "liberar" o benefício.

COMO ACONTECE

A mensagem chega por WhatsApp, SMS, e-mail ou rede social, muitas vezes encaminhada por um conhecido. Pede para responder uma pesquisa, compartilhar com amigos e pagar um frete ou taxa simbólica. Os dados coletados são usados em outros golpes.

COMO PREVENIR

- Confira o cupom ou a promoção no site ou no aplicativo oficial da loja.
- Loja de verdade não cobra para entregar prêmio nem pede senha ou código para liberar cupom.
- Não compartilhe a mensagem com outras pessoas antes de conferir.

SE JÁ ACONTECEU

1. Se pagou ou digitou o cartão, ligue para o banco e peça o bloqueio e a contestação.
2. Se informou CPF e outros dados pessoais, fique atento a mensagens e ligações que usem esses dados para parecer confiáveis.
3. Se informou senha ou código, troque as senhas e ative a autenticação de dois fatores.

4. Avise quem mandou a mensagem para você, para que não continue encaminhando.

8

Falsa central de atendimento.

Depois da compra, alguém liga ou manda mensagem se passando pela loja ou pelo banco, fala de um problema no pagamento e pede código, senha ou um novo Pix.

O QUE É

Depois de uma compra real, alguém liga ou manda mensagem se passando pela loja ou pelo banco. Fala de um problema no pagamento, de uma compra suspeita ou de um estorno, e pede código, senha ou um novo Pix.

COMO ACONTECE

O golpista pode já ter seu nome, CPF e os dados da compra, vazados ou coletados em outros golpes, o que deixa a conversa convincente. Pede para você confirmar um código recebido por SMS, instalar um aplicativo de "suporte" ou fazer um Pix para uma "conta de segurança".

COMO PREVENIR

- Banco e loja não pedem senha, código recebido por SMS nem Pix para "proteger" ou "estornar" dinheiro.
- Desligue e ligue você mesmo para o número oficial que está atrás do cartão ou no aplicativo.
- Não instale aplicativo a pedido de quem ligou.

SE JÁ ACONTECEU

1. Desligue e ligue para o banco pelo número oficial. Peça o bloqueio do cartão e das transações.
2. Se fez um Pix, peça a abertura do MED.
3. Se informou senha ou código, troque as senhas do banco e do e-mail a partir de outro aparelho e confira se não houve outras transações.
4. Se instalou um aplicativo a pedido do golpista, desinstale e, se tiver dúvida, siga o guia "Celular hackeado" deste site.
5. Registre um boletim de ocorrência.

PARTE 2



Como conferir se a loja é real antes de pagar

- 1 Digite o endereço da loja você mesmo**, em vez de clicar em anúncio, link de mensagem ou e-mail.
- 2 Confira o endereço com atenção.** Letra trocada, hífen a mais ou um nome parecido com o da marca são sinais de site falso. O cadeado no navegador só mostra que a conexão é protegida; site falso também tem cadeado.
- 3 Procure o CNPJ no rodapé do site** e consulte na Receita Federal. Confira se a empresa existe, se está ativa e se o nome bate com o da loja.
- 4 Pesquise a reputação** da loja em sites de reclamação e veja como ela responde aos clientes. Loja sem nenhuma reclamação e sem nenhum histórico também é sinal de alerta.
- 5 Compare o preço** em outras lojas grandes. Se só uma loja tem o produto pela metade do preço, desconfie.
- 6 Desconfie de loja sem contato real:** sem telefone, sem endereço, só com formulário ou só com WhatsApp.
- 7 Acompanhe o preço com antecedência.** Anote o valor dos produtos que você quer nas semanas anteriores, para saber se o desconto da Black Friday é verdadeiro.

PARTE 3



Como pagar com mais segurança

- 1 Prefira o cartão de crédito**, de preferência o cartão virtual do aplicativo do banco. Ele permite contestar a compra e pode ser cancelado depois.
- 2 Pix só para lojas que você conferiu**, e confira o nome do recebedor antes de confirmar. O nome tem que ser o da empresa, não o de uma pessoa.
- 3 Nunca pague taxa para liberar entrega, cupom ou prêmio** por link recebido em mensagem.
- 4 Guarde tudo:** prints do anúncio, da página do produto, do pedido, do comprovante e das conversas.
- 5 Use a autenticação de dois fatores** no e-mail e no aplicativo do banco, e ative os avisos de compra no celular.

PARTE 4



Se você já caiu no golpe

- 1 Ligue para o banco imediatamente** pelo número que está atrás do cartão ou dentro do aplicativo. Peça o bloqueio do cartão e a contestação da compra.
- 2 Se pagou por Pix, peça ao banco a abertura do Mecanismo Especial de Devolução (MED).** Quanto antes, maior a chance de o dinheiro ainda estar na conta do golpista.
- 3 Registre um boletim de ocorrência**, que pode ser feito pela delegacia eletrônica do seu estado. Ele ajuda na contestação com o banco.

- 4 **Se informou senha ou código**, troque as senhas do banco e do e-mail a partir de outro aparelho e confira se não houve outras transações.
- 5 **Denuncie a loja ou o perfil falso** na rede social onde viu o anúncio e registre a reclamação nos canais de defesa do consumidor.
- 6 **Avise seus contatos**, porque o mesmo golpe costuma circular entre amigos e família.

MENSAGEM PRONTA PARA AVISAR SEUS CONTATOS

Pessoal, cuidado com lojas e anúncios de Black Friday com preço bom demais. Antes de pagar, confirmem o endereço do site, o CNPJ da loja e o nome de quem vai receber o Pix. Na dúvida, prefiram o cartão de crédito. Eu quase caí em um golpe assim.

DÚVIDAS COMUNS

Perguntas frequentes

? Como saber se um site é confiável?

Digite o endereço da loja você mesmo e confira o endereço letra por letra. Procure o CNPJ no rodapé e consulte na Receita Federal, pesquise a reputação da loja em sites de reclamação, compare o preço com outras lojas grandes e desconfie de loja sem telefone nem endereço.

? O cadeado no navegador garante que o site é seguro?

Não. O cadeado só mostra que a conexão é protegida. Site falso também tem cadeado.

❓ **É seguro pagar com Pix na Black Friday?**

Use o Pix só em lojas que você conferiu e confira o nome do recebedor antes de confirmar: tem que ser o da empresa, não o de uma pessoa. Sempre que puder, prefira o cartão de crédito, de preferência o cartão virtual do aplicativo do banco, que permite contestar a compra.

❓ **Caí em um golpe de loja falsa. O que fazer?**

Ligue para o banco imediatamente, pelo número atrás do cartão ou dentro do aplicativo, e peça o bloqueio do cartão e a contestação da compra. Se pagou por Pix, peça a abertura do MED. Registre um boletim de ocorrência, troque as senhas se informou senha ou código e denuncie a loja ou o perfil falso.

❓ **Como pedir de volta um Pix feito para um golpista?**

Peça ao banco a abertura do Mecanismo Especial de Devolução (MED), pelo aplicativo, na área do Pix, ou pela central. O pedido pode ser feito em até 80 dias depois do Pix, mas quanto antes, maior a chance de o dinheiro ainda estar na conta do golpista. O MED não garante a devolução: o banco do golpista bloqueia o que ainda houver na conta e analisa o caso.

❓ **Quando é a Black Friday de 2026?**

A Black Friday de 2026 cai em 27 de novembro. As semanas antes dela são as preferidas dos golpistas.

Precisa de ajuda?

A JAL Softwares, por meio da Vortex CyberSegurança, ajuda a conferir se uma loja ou um link é confiável e orienta quem caiu em golpe 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: 19 de outubro de 2026.