Editor: José Carlos Vieira (Cidades)
josecarlos.df@dabr.com.br
Tels. : 3214-1119/3214-1113
Atendimento ao leitor: 3342-1000
cidades.df@dabr.com.br

86%
dos consumidores desistiram de aproveitar uma promoção por medo de cair em golpes digitais

29.689
tentativas de fraude identificadas no e-commerce em apenas quatro dias de Black Friday (27 a 30 de novembro de 2025)

R$ 30,7
milhões em prejuízos evitados após o bloqueio das tentativas de fraude no período

R$ 1.034,77
em cada tentativa de transação suspeita, quantia 45,44% superior à média dos pedidos legítimos (R$ 564,57)

71,6%
das ocorrências de tentativas de fraude nas Gerações Y (39%) e Z (32,6%)

1,41%
de compras fraudulentas no Natal, valor quase três vezes superior ao registrado na Black Friday (0,50%)

9.545
tentativas na sexta-feira de Black Friday, associado a R$ 11,18 milhões em fraudes

SEGURANÇA

Alerta para golpes nas compras de fim de ano

Levantamento da Serasa Experian revela que o medo de fraudes afasta 86% consumidores de promoções. Natal lidera em proporção de ameaças, e as gerações Y e Z concentram mais de 70% das investidas em datas como a Black Friday

» CARLOS SILVA
» ANA CAROLINA ALVES

O medo de cair em um golpe digital fez 86% dos consumidores desistirem de aproveitar uma promoção. Em apenas quatro dias de Black Friday, entre 27 e 30 de novembro de 2025, foram identificadas 29.689 tentativas de fraude no comércio eletrônico. As ocorrências poderiam ter provocado um prejuízo de R$ 30,7 milhões, caso não tivessem sido barradas. Com a aproximação das festas de fim de ano, quando a procura por eletrônicos, roupas e outros produtos aumenta, os criminosos encontram novas oportunidades para explorar a pressa e a expectativa dos compradores, que se encontram entre o receio e a oferta.

O Mapa da Fraude da Serasa Experian identificou uma média de 7.422 tentativas de fraude por dia durante os quatro dias analisados — aproximadamente 309 investidas por hora. O levantamento também chama a atenção para o valor das transações suspeitas: o valor médio em cada uma das tentativas chegou a R$ 1.034,77, quantia 45,44% superior à média registrada entre os pedidos legítimos (R$ 564,57).

Uma pesquisa de opinião realizada pela Serasa Experian em setembro deste ano, com 1.480 entrevistados, identificou quais ameaças mais preocupam os brasileiros durante períodos de grandes promoções. Os sites falsos aparecem no topo da lista, mencionados por 53% dos participantes. Na sequência, estão os golpes envolvendo pagamentos via Pix, citados por 42%, e os anúncios fraudulentos em redes sociais, apontados por 32%.

Datas e idades

Embora a Black Friday concentre um volume expressivo de transações, o Natal apresenta uma proporção maior de tentativas de fraude em relação aos pedidos realizados. Segundo o levantamento da Serasa Experian, 1,41% das compras feitas no período natalino foram classificadas como tentativas fraudulentas. O índice é praticamente três vezes superior ao registrado na Black Friday, que apresentou percentual de 0,50%.

A comparação considera diferentes datas comemorativas do calendário comercial. O Natal aparece entre os períodos com maior proporção de tentativas de fraude, atrás apenas da Páscoa, que registrou 1,42%. Na sequência estão Dia das Mães (1,26%), Dia dos Namorados (1,08%), Dia das Crianças (1,08%) e Dia dos Pais (1,07%).

A sexta-feira da Black Friday, no entanto, foi o dia com maior número de tentativas de fraude durante o período analisado pela Serasa Experian. Em 28 de novembro de 2025, foram identificadas 9.545 ocorrências, associadas a R$ 11,18 milhões. O volume representa a maior concentração diária de tentativas entre os cinco dias considerados no levantamento, que também inclui a Cyber Monday.

Na quinta-feira anterior à Black Friday, foram registradas 7.903 tentativas, com R$ 8,14 milhões associados. No sábado, o número chegou a 6.322 ocorrências, enquanto o domingo contabilizou outras 5.919. Na Cyber Monday, em 1º de dezembro, foram identificadas 6.595 tentativas, que poderiam representar R$ 6,68 milhões em prejuízos.

Além da quantidade de ocorrências, o valor médio das transações suspeitas também chama a atenção. Na sexta-feira da Black Friday, o ticket médio das tentativas chegou a R$ 1.171,59, o maior entre os dias analisados. Na quinta-feira, a média foi de R$ 1.030,50. No sábado, caiu para R$ 1.008,01 e, no domingo, chegou a R$ 848,40. Na Cyber Monday, o valor médio ficou em R$ 1.014,20.

Os dados também apontam diferenças entre as faixas etárias. As gerações Y (nascidos entre 1981 e 1996) e Z (de 1997 a 2010) concentraram juntas 71,6% das tentativas de fraude identificadas durante a Black Friday de 2025, considerando os registros com informação de idade.

A geração Y liderou o levantamento, com 8.092 tentativas, o equivalente a 39% do total analisado. O ticket médio das operações suspeitas foi de R$ 1.116,36. A geração Z foi responsável por 6.766 ocorrências, ou 32,6%, com valor médio de R$ 880,83.

Já a geração X (nascidos entre 1965 e 1980) respondeu por 18,7% das tentativas, com 3.866 registros e ticket médio de R$ 1.157,94. Entre os baby boomers (nascidos entre 1946 e 1964), foram identificadas 1.694 ocorrências, correspondentes a 8,2% do total.

A estudante Ana Clara Diniz, 24 anos, perdeu cerca de R$ 70 após encontrar em uma rede social um anúncio de um kit de produtos para beleza. "Várias pessoas postaram, com vários comentários dizendo que era aquilo ali e tudo mais. Tinha um preço interessante, mas não era um preço tão abaixo do mercado", conta. Depois de realizar o pagamento, ela começou a receber novas cobranças, supostamente relacionadas à entrega e ao transporte do produto, que nunca recebeu.

A recomendação de Ana Clara para quem pretende aproveitar as promoções de fim de ano é conferir a procedência das ofertas e buscar informações nos canais oficiais das empresas. "É bom sempre procurar nos sites oficiais, ver realmente se aquilo é de verdade", aconselha.

Em uma negociação realizada por um site de compras, a profissional de audiovisual e fotografia Jéssica da Silva, 23, adquiriu uma bolsa e uma carteira, mas os produtos nunca chegaram. Apesar de tentar resolver a situação pelos canais da própria plataforma, não conseguiu recuperar o dinheiro nem localizar novamente a loja responsável pela venda.

"Eu corri atrás pela própria plataforma, não tive retorno nenhum. A pessoa sumiu, nunca mais vi a loja dela", relembra. Jéssica estima que tenha perdido entre R$ 150 e R$ 200 na negociação, e concorda que a aparência cada vez mais convincente das fraudes amplia a vulnerabilidade dos consumidores. "Meus pais também caíram em vários golpes por conta da inteligência artificial. Hoje, quem cuida das compras deles sou eu, justamente para eles não caírem mais", frisa.

Quem paga a conta

A vítima de um golpe digital nem sempre precisa arcar sozinha com o prejuízo. É o que explica André Borini Ferreira Dias, diretor de Atendimento do Procon-DF. Mas é preciso lembrar também que a simples ocorrência de uma fraude não significa que a instituição será automaticamente obrigada a ressarcir o consumidor. "É preciso analisar como a fraude aconteceu e se houve falha na segurança ou na prestação do serviço", afirma.

Entre as situações que podem gerar responsabilização estão a autorização de movimentações incompatíveis com o perfil do cliente, a ausência de mecanismos de bloqueio e confirmação de operações e a abertura ou manutenção de contas utilizadas para aplicar golpes. A instituição também pode responder quando não toma providências adequadas depois de ser comunicada sobre uma fraude.

Além de estar atento aos direitos na hora de cobrar a instituição financeira, algumas compras requerem mais atenção. Na aquisição de passagens aéreas e aluguéis de temporada, a orientação é redobrar o cuidado. "Antes de pagar, o consumidor deve comparar o valor em empresas conhecidas, digitar o endereço do site diretamente no navegador e conferir se está no canal oficial, sem confiar apenas no link recebido por mensagem ou em um perfil de rede social."

A aparência de uma loja conhecida nem sempre é garantia de segurança na hora de comprar pela internet. O alerta é de Washington Bruno, diretor de Operações da Globalweb. Segundo o especialista, os consumidores devem observar atentamente a URL antes de informar dados pessoais ou financeiros. "A falsificação geralmente está no endereço eletrônico, com pequenas alterações na URL original, como a adição de letras, números ou palavras que passam despercebidas em uma leitura rápida", explica.

A rapidez do Pix, que facilita as compras pela internet, também exige cuidados adicionais. Antes de confirmar a operação, é necessário conferir o nome e os dados bancários apresentados pelo aplicativo. "Se o beneficiário for uma pessoa física desconhecida ou uma empresa diferente daquela em que a compra foi realizada, é melhor interromper a transação e investigar", frisa.

Caso perceba que foi vítima de um golpe, a orientação é procurar imediatamente o banco ou a instituição financeira para comunicar a fraude e solicitar as providências cabíveis. A rapidez na comunicação pode ajudar a minimizar os prejuízos. "A segurança digital é uma responsabilidade compartilhada entre empresas, plataformas e consumidores. A tecnologia oferece cada vez mais recursos de proteção, mas a conscientização continua sendo uma das nossas principais ferramentas contra os golpes."



Carlos Silva/CB/D.A.Press



Ana Clara Diniz e Jéssica da Silva foram vítimas de fraudes no e-commerce

Atenção para as dicas

Confira a barra de endereço antes de digitar dados pessoais ou bancários. Golpistas usam alterações sutis (letras trocadas, números ou palavras extras) para imitar marcas conhecidas

- O protocolo com ícone de cadeado garante criptografia na conexão, mas páginas fraudulentas também usam o recurso;
- Evite acessar lojas através de links recebidos por redes sociais, aplicativos de mensagem ou anúncios patrocinados — pesquise a loja diretamente nos buscadores;
- Desconfie de falhas de português, informações incompletas sobre a empresa, ausência de canais oficiais de suporte e preços excessivamente abaixo do valor de mercado;
- Antes de confirmar qualquer transferência via Pix, certifique-se de que o nome, CPF/CNPJ e instituição bancária pertencem de fato à loja ou empresa contratada, e não a terceiros/pessoas físicas desconhecidas;
- Pressa imposta para fechar o negócio ou ofertas discrepantes são os principais indicativos de fraude;
- Verifique a regularidade de agências de turismo no cadastro do Ministério do Turismo (Cadastur);
- Entre em contato o mais rápido possível com o banco ou instituição financeira de origem para comunicar o ocorrido e bloquear novos acessos.

Fonte: André Borini Ferreira Dias, diretor de Atendimento do Procon-DF, e Washington Bruno, diretor de Operações da Globalweb