Bolsas
Na quinta-feira: 0,61% São Paulo
Na sexta-feira: 1,93% Nova York

Pontuação B3
IBovespa nos últimos dias
171.336 — 166.376
16/11 17/11 18/11 19/11

Na quinta-feira
R$ 5,934
(+1,15%)

Dólar

	Últimos
12/novembro	5,586
13/novembro	5,654
16/novembro	5,776
17/novembro	5,782
18/novembro	5,866

Salário mínimo
R$ 1.621

Euro
Comercial, venda na quinta-feira
R$ 6,512

CDI
Ao ano
13,65%

CDB
Prefixado 30 dias (ao ano)
13,68%

Inflação
IPCA do IBGE (em %)

Junho/2026	0,16
Julho/2026	0,07
Agosto/2026	-0,32
Setembro/2026	0,82
Outubro/2026	0,14

BLACK FRIDAY

Avanço da inteligência artificial torna fraudes mais sofisticadas, enquanto instabilidade em lojas virtuais pode direcionar compradores a páginas falsas. Especialistas alertam para impactos econômicos e defendem reforço da segurança digital

GOLPES DIGITAIS ameaçam consumidores

» FERNANDA STRICKLAND

A proximidade da Black Friday, em 27 de novembro, e das compras de Natal acendem o alerta para o avanço das fraudes digitais. Com inteligência artificial (IA), criminosos criam anúncios, mensagens e páginas falsas mais convincentes, dificultando a identificação de golpes. Além dos prejuízos financeiros, as fraudes ameaçam a confiança dos consumidores e podem afetar as vendas de empresas legítimas.

Dados da Serasa Experian apontam que, entre 27 e 30 de novembro de 2025, foram registradas 29.689 tentativas de fraude em pedidos de comércio eletrônico, com R$ 30,7 milhões em prejuízos potenciais. O aumento das transações amplia as oportunidades para criminosos, que recorrem a lojas virtuais clonadas, QR Codes adulterados e roubo de credenciais.

Para o economista Otto Nogami, professor do Instituto de Ensino e Pesquisa (Insper), o problema vai além da segurança individual e afeta o funcionamento do mercado. A dificuldade de identificar ofertas legítimas amplia a assimetria de informação entre compradores e vendedores, aumenta os custos de transação e prejudica a eficiência econômica.

A desconfiança também afeta empresas que atuam corretamente. Ao questionar a autenticidade das promoções, o consumidor passa mais tempo verificando preços, vendedores e condições de pagamento. Com isso, ofertas legítimas podem perder espaço para anúncios fraudulentos aparentemente mais vantajosos.

O comportamento dos consumidores também é afetado. Contagens regressivas, mensagens de urgência, descontos elevados e falsas indicações de estoque limitado estimulam decisões precipitadas ao explorar a aversão à perda e a sensação de oportunidade passageira.

Assim, as fraudes não provocam apenas perdas financeiras, mas também reduzem o número de transações pela falta de confiança. O problema prejudica a concorrência e aumenta os custos das empresas com mecanismos adicionais de proteção.

Sofisticação

Para Rodolfo Oliveira, advogado da área de Meios de Pagamentos e Fintechs do escritório Barcellos Tucunduva Advogados, o aumento das transações durante a Black Friday amplia o espaço para a atuação de criminosos. "A inteligência artificial amplia a capacidade de produzir abordagens convincentes e automatizar ataques", explica.

Entre os principais riscos estão a falsificação de lojas e anúncios, o roubo de credenciais e o direcionamento de pagamentos para contas controladas por fraudadores. Uma das práticas recorrentes envolve QR Codes adulterados, que podem direcionar o dinheiro para destinatários diferentes dos anunciados.

O advogado Luiz Fernando Plastino, especialista em Propriedade Intelectual, Privacidade e Proteção de Dados e Direito de Informática, também do escritório Barcellos Tucunduva Advogados, recomenda conferir as informações do recebedor antes de concluir qualquer pagamento. "Os QR Codes de Pix devem levar ao aplicativo normal de pagamento, não para um website e, principalmente, não devem trazer arquivos para download", alerta.

A engenharia social também é usada em golpes. Com dados pessoais das vítimas, criminosos enviam mensagens falsas sobre entregas, cobranças e pendências em pedidos para induzir o acesso a links fraudulentos ou pagamentos indevidos.

Plastino recomenda acompanhar as compras apenas pelos canais oficiais das lojas e desconfiar de solicitações inesperadas. Ele ressalta que a Lei Geral de Proteção de Dados (LGPD) e o Código de Defesa do Consumidor estabelecem obrigações de segurança e proteção de dados. A responsabilização das empresas, porém, depende das circunstâncias, das medidas adotadas e da relação entre eventuais falhas e os prejuízos. "Não é qualquer vazamento de dados que automaticamente vai levar à responsabilização", esclarece.

Ataques

O risco vai além das fraudes contra consumidores. Às vésperas da Black Friday, o comércio eletrônico também enfrenta ataques à infraestrutura tecnológica, capazes de instabilizar sistemas nos períodos de maior movimento.

Os professores Jéferson Nobre e Alberto Schaeffer Filho, do Instituto de Informática da Universidade Federal do Rio Grande do Sul (UFRGS), alertam para duas frentes de atuação dos criminosos: fraudes contra consumidores e ataques aos sistemas das varejistas.

Entre as estratégias estão o uso de redes de dispositivos comprometidos, conhecidas como botnets, e de proxies residenciais, que dificultam a identificação de atividades maliciosas. Ataques relâmpago, que duram menos de um minuto, podem provocar instabilidade na finalização das compras e perdas imediatas de receita.

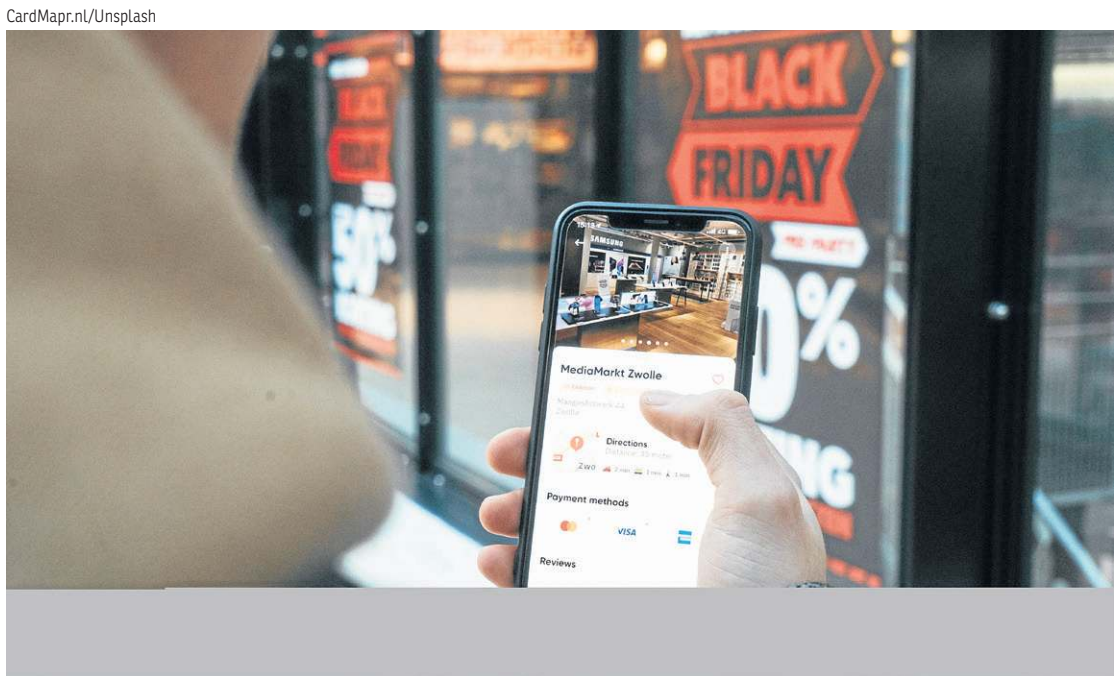
A instabilidade também pode levar consumidores a buscar o produto em outras lojas por meio de buscadores e redes sociais, aumentando a exposição a anúncios falsos, domínios clonados e páginas criadas para roubar dados e interceptar pagamentos.

A inteligência artificial tem papel duplo nesse cenário: ajuda a identificar vulnerabilidades e proteger sistemas, mas também facilita a criação de ferramentas para ataques.

Um dos pontos de atenção é o chamado vibe coding, prática de desenvolver sistemas e páginas por meio de comandos em linguagem natural para ferramentas de IA. O professor Jéferson Nobre alerta que um sistema funcional não é necessariamente seguro. Dados da Veracode indicam que 45% das amostras de código geradas por IA apresentam vulnerabilidades críticas relacionadas ao OWASP Top 10.

Os professores defendem que o varejo também incorpore IA aos mecanismos de defesa, com identificação automatizada de vulnerabilidades, retirada antecipada de domínios falsos do ar e respostas mais rápidas a ataques.

CardMapr.nl/Unsplash



Período promocional favorece golpes virtuais, como lojas falsas, QR Codes adulterados e roubo de dados

Como se proteger

Especialista dá recomendações e práticas ao consumidor para que ele não caia em fraudes

» Pesquise o histórico de preços. Compare o preço atual com o praticado nas semanas anteriores. Um desconto de 50% pode ser ilusório se o preço tiver sido elevado artificialmente antes da promoção.

» Desconfie de ofertas excessivamente vantajosas. Preços muito inferiores aos encontrados no mercado podem indicar produtos falsificados, lojas fraudulentas ou golpes.

» Verifique a reputação da loja. Consulte o CNPJ, os canais de atendimento e os registros de reclamações. Dê preferência a fornecedores conhecidos ou com histórico verificável.

» Evite comprar por links recebidos em mensagens. Golpistas frequentemente utilizam WhatsApp, SMS, redes sociais e anúncios patrocinados para direcionar consumidores a páginas falsas. Acesse o site oficial digitando o endereço.

» Confira o endereço eletrônico. Verifique se o domínio corresponde à loja verdadeira. O cadeado e o protocolo HTTPS indicam uma conexão criptografada, mas não garantem que o vendedor seja legítimo.

» Tenha cuidado com pagamentos via Pix. Confira o nome e os dados do destinatário antes de confirmar. Desconfie quando uma loja desconhecida exige pagamento exclusivamente por Pix ou transferência.

» Compare o preço total da compra. Frete, taxas e condições de entrega podem eliminar a vantagem do desconto anunciado.

» Evite o endividamento por impulso. Parcelas aparentemente pequenas podem comprometer a renda futura. Considere o custo total da compra e eventuais juros do financiamento.

» Conheça seus direitos. Nas compras realizadas pela internet, o Código de Defesa do Consumidor prevê, em regra, o direito de arrependimento em até sete dias após o recebimento do produto.

» Guarde os comprovantes. Salve anúncios, capturas de tela, confirmação do pedido, condições de pagamento e prazo de entrega. Esses registros podem ser fundamentais em eventuais reclamações.

Fonte: Economista Otto Nogami, professor do Instituto de Ensino e Pesquisa (Insper), Secretaria Nacional do Consumidor e dos Procons.

PO NEWS
Boletim informativo das Organizações PauloOctavio
Informe publicitário
EDIÇÃO Nº 1080 | ANO 51
22 DE NOVEMBRO DE 2026 | BRASÍLIA/DF



JK SHOPPING 13 ANOS
EMPREENDIMENTO CELEBRA ANIVERSÁRIO COM EXPOSIÇÃO EM HOMENAGEM A JUSCELINO KUBITSCHEK

O JK Shopping comemorou seus 13 anos com a inauguração de uma exposição dedicada ao ex-presidente Juscelino Kubitschek, em parceria com o Memorial JK. Instalada no JK Espaço Arte, a mostra reúne registros e conteúdos sobre a trajetória do fundador de Brasília e ficará aberta ao público até 19 de janeiro de 2027.

A exposição conta com uma atividade interativa: uma mesa de desenho na qual crianças e adultos podem reproduzir imagens inspiradas na história e nas paisagens da Capital, levando suas produções para casa. A iniciativa busca aproximar diferentes gerações da memória de Brasília.

Para o empresário Paulo Octávio, a homenagem representa o reconhecimento de um legado que continua inspirando a cidade. A programação também marca a inauguração de um teatro com capacidade para 200 pessoas, que passa a integrar o JK Espaço Arte, ampliando a oferta de espetáculos, apresentações musicais, palestras e encontros culturais.

www.paulooctavio.com.br