GOLPES de sites e emails falsos de Black Friday triplicaram desde outubro; saiba como evitar

Dois a cada três consumidores brasileiros pretendem ir às compras na Black Friday atrás de boas ofertas, de acordo com dados do Google. Nos últimos novembros, estelionatários têm surfado nessa onda para enganar pessoas na internet.

O site falso ‘Loja Estoque Brasil, por exemplo, colocou um grande banner genérico com anúncios de descontos de até 30%. No catálogo do portal, é possível encontrar uma caixa de som JBL Boombox, vendida em geral a preços por volta de R$ 2.000, por R$ 247,99.

Sozinho, o desconto de 88% gera desconfiança. Ao rolar a página até o fim, o comprador ainda pode encontrar outros indícios preocupantes: o email de contato "supore@estoquedobrasi.com" (sem "t") e o endereço "Rua Alameda, 123 Bairro Santo André, São Paulo."

Reclamações na rede social Reddit e no portal de queixas de consumidores Reclame Aqui corroboram as suspeitas. Neste último, há 12 reclamações no último mês —todas sem resposta.

Relatório da empresa de cibersegurança Kaspersky mostra que o caso da Loja Estoque Brasil é um entre muitos. O documento mostra aumento de três vezes nos sites falsos usando o termo "Black Friday" desde outubro. Esses ataques são chamados por especialistas de phishing, em referência à palavra pescaria em inglês, já que os cibercriminosos usam algum tema de interesse como isca.

Os sites e emails falsos são a tática mais adotada no Brasil por estelionatários para aplicar golpes. Nos primeiros dez meses de 2023, a Kaspersky identificou e bloqueou mais de 30 milhões de ataques de phishing voltados a compras online, sistemas de pagamento e instituições bancárias.

Itens de alta procura na data, como eletrônicos, são iscas recorrentes em golpes na Black Friday. A Kaspersky encontrou 2,8 milhões de ataques de phishing de janeiro a outubro de 2023 só com menções a iPhones e outros produtos e serviços da Apple. Outra variação de golpe é direcionada aos gamers de console com ofertas de jogos, mas que no fim, só servem para deixar os jogadores com os bolsos vazios.

Embora pareça um esquema grosseiro, esse golpe é recorrente porque funciona, dizem os especialistas em segurança ouvidos pela reportagem. As plataformas de comércio eletrônico foram usadas como disfarce em 43,5% das mensagens falsas.

Os estabelecimentos golpistas podem aparecer em marketplaces, como Google Shopping, Amazon e Mercado Livre. Por isso, o consumidor precisa se proteger conferindo qual a loja responsável pela venda, já que muitas vezes a plataforma não faz a venda diretamente.

Esses sites, em geral, têm protocolos de atendimento para contornar calotes e desacordos

entre as partes envolvidas na negociação, mas o responsável por efetuar estornos ou resolver problemas de entrega é o vendedor.

Especialistas aconselham que as pessoas verifiquem o histórico das lojas no Google e em sites de queixa como o Reclame Aqui. Do lado das plataformas, há incentivos para denunciar os vendedores de má conduta —desde fraudes a problemas de atendimento.

O diretor da área de fraude e risco da empresa de pagamento Pomelo, Gilmar Magi, recomenda que as pessoas prefiram fazer pagamento via cartão de crédito ou débito, uma vez que é possível contestar a operação. "*O cliente pode ligar para o banco emissor, informar o problema, uma entrega que nunca aconteceu, por exemplo, e iniciar uma disputa sobre a validade dessa transação*."

No caso do Pix, os bancos têm sistemas para indicar transferências com maior risco de fraude para alertar o cliente. Há chances menores do que no cartão, mas é possível solicitar estorno dos valores, caso a fraude seja comprovada. O pagamento via boleto, por sua vez, não é ressarcido, segundo Magi.

O cliente também deve preferir gerar cartões virtuais para realizar compras na internet. Nessa modalidade, o banco gera dados para pagamento usados somente naquela compra, o que diminui a chance de vazamento de dados sensíveis.

Ainda antes disso, o consumidor deve checar o nome do site com cuidado. Segundo a Febraban (Federação Brasileira de Bancos), criminosos também clonam sites de varejistas famosos para induzir os consumidores ao erro, colocando uma letra a mais no endereço do site, que muitas vezes fica imperceptível para o cliente ou ainda trocando, por exemplo, uma letra "o" pelo número "0".

"*Por isso, recomendamos que o cliente faça sua pesquisa de preços, e quando escolher a loja, digite diretamente o endereço do site na barra do navegador. Nunca clique em links enviados por e-mails, SMS ou aplicativos de mensagens e sempre dê preferência para lojas conhecidas*", diz Adriano Volpini, diretor do comitê de prevenção a fraudes da Febraban.

O diretor também alerta sobre lojas recentes com todos os depoimentos de compradores positivos em redes sociais. "*Golpistas criam perfis falsos que investem em mídia para aparecer em páginas e stories de redes sociais, inclusive com depoimentos falsos de compradores. Também usam sites de vendedores de depoimentos e bancos de fotos e vídeos internacionais para dar crédito ao produto e enganar o consumidor*."

A Kaspersky, em seu relatório, também alerta sobre cartões de presente falsos. "*Por exemplo, um site falso imita uma conhecida loja online, seduzindo os internautas com cartões de presente de € 800 a € 1,95. Como normalmente esses cartões não existem, as vítimas novamente perdem seu dinheiro*."

Veja 10 dicas de segurança para esta Black Friday:

1 Dar preferência aos sites conhecidos para as compras e verificar a reputação de sites não conhecidos em páginas de reclamações

2 Ter muito cuidado com e-mails de promoções que tenham links. Ao receber um e-mail não

solicitado, verificar se realmente se trata de uma empresa idônea. Acessar o site digitando os dados no navegador e não clicando em links

3 Sempre desconfiar de empresas que pedem pagamentos antecipados e prometem entregas em prazos longos

4 Verificar com atenção as formas de pagamento oferecidas pelo e-commerce e desconfiar quando existem poucas opções

5 Desconfiar das promoções cujos preços sejam muito menores que o valor real do produto

6 Verificar se a página tem selo de autenticação e número de seguidores compatíveis. Desconfiar de páginas recém-criadas

7 Dar preferência para o uso de cartão virtual nas compras online

8 Se for fazer uma compra presencial com cartão, sempre conferir o valor na maquininha de cartão antes de digitar a sua senha

9 Em caso de compras presenciais, insirir você mesmo o cartão na maquininha. Caso tenha entregado o cartão ao vendedor, sempre verificar se o cartão devolvido é realmente o seu

10 Se for pagar com Pix, sempre fazer o pagamento dentro do ambiente da loja virtual. Quando o varejista fornecer o código QR Code, conferir com atenção todos os dados do pagamento e se a loja escolhida é realmente quem irá receber o dinheiro. Só fazer a transferência após essa checagem detalhada. A mesma dica vale para pagamentos com boletos

Foto: Divulgação