

Melpomenem_CANVA



GOLPES NA BLACK FRIDAY

POR QUE PROTEGER A IDENTIDADE DA MARCA VIROU PRIORIDADE?

A Black Friday concentra não apenas um dos maiores volumes de ofertas do ano, mas também condições especialmente favoráveis para golpes digitais.

Carlos Feist (*)

Em sua edição de 2025, uma pesquisa específica conduzida pelo Reclame Aqui constatou que 76% dos consumidores se sentiam inseguros ou desconfiados diante da possibilidade de golpes elaborados com IA, além de 63% que não sabiam identificar uma tentativa nesse sentido com essa tecnologia.

Nesse cenário, o problema deixa de ser apenas educar o consumidor a desconfiar: é preciso construir uma infraestrutura de comunicação capaz de provar que uma mensagem realmente veio da marca que afirma representar, protegendo sua identidade, reputação e, com isso, criando um ecossistema favorável para um ROI positivo. Até porque, o golpe se esconde, justamente, no volume.

Durante a Black Friday, o consumidor recebe dezenas de ofertas por dia, de empresas conhecidas e desconhecidas. Ele já espera obter cupons, links de pagamento, confirmações de compra e códigos de rastreio. Por isso, o criminoso não precisa necessariamente criar uma situação estranha. Basta reproduzir, com precisão, aquilo que o cliente já está esperando acontecer.

É essa combinação que torna a data tão atraente para criminosos digitais: urgência, desconto e volume. A mensagem de "só hoje" reduz o tempo dedicado à desconfiança, enquanto uma oferta agressiva parece plausível justamente durante a temporada promocional. Do outro lado, o custo para disparar mensagens em massa e criar páginas ou links falsos é baixo. O golpe, portanto, encontra, na própria dinâmica comercial da Black Friday, um ambiente favorável para prosperar.

O problema é que a responsabilidade pela identificação de uma fraude não pode recair exclusivamente sobre quem recebe a mensagem. É claro que o consumidor tem um papel importante: desconfiar de urgências exageradas e verificar a origem antes de clicar. Mas, ele não pode ser transformado na última linha de defesa de um ecossistema de comunicação que é controlado pelas empresas e pelas plataformas.

Há, inclusive, um interesse direto do negócio nessa discussão. Quando um cliente cai em um golpe em nome de uma determinada marca, o prejuízo não termina na transação fraudulenta. A empresa pode ter de lidar com atendimento, reclamações e perda de confiança. Afinal, na percepção do consumidor, o problema está associado à marca que ele acredita ter enviado aquela comunicação, e não necessariamente ao criminoso que a falsificou.



Divulgação

Carlos Feist

> "A verificação precisa entrar no planejamento da campanha desde o início, inclusive no orçamento, como uma linha de performance ao lado da mídia. Perfis verificados e mecanismos de autenticação de voz dependem de processos de homologação e aprovação externa.

Isso cria um efeito ainda mais amplo, prejudicando a comunicação legítima. Quando o consumidor passa a desconfiar de todas as mensagens, ele pode ignorar uma oferta verdadeira, deixar de clicar em um link legítimo ou não atender uma ligação real da empresa. Cria-se, assim, uma espécie de "taxa de desconfiança" que incide sobre toda a operação, reduzindo a resposta e encarecendo a conversão.

É por isso que a verificação do remetente precisa deixar de ser tratada como um recurso adicional de segurança e passar a fazer parte da própria infraestrutura de comunicação das marcas. Na prática, a empresa precisa chegar à Black Friday com uma identidade reconhecível nos canais em que conversa com seus clientes.

No WhatsApp, isso significa utilizar um perfil com selo oficial da Meta. No RCS, proporcionar uma experiência segura na caixa de mensagens, com nome, logotipo e selo verificado pelo Google, além de imagens e botões. No SMS, o uso de número curto dedicado ajuda a estabelecer uma origem reconhecível e um alcance maior. Na comunicação por voz, mecanismos como STIR/SHAKEN e a Origem Verificada da Anatel permitem autenticar a identidade da empresa e reforçar, para o consumidor, quem está do outro lado da ligação.

O ponto comum entre essas alternativas é justamente a participação de terceiros na validação da identidade — como Meta, Google e operadoras. Isso dificulta a reprodução da identidade por criminosos e, principalmente, cria consistência na jornada. Essa preparação, entretanto, não pode começar quando os golpes já estiverem circulando.

A verificação precisa entrar no planejamento da campanha desde o início, inclusive no orçamento, como uma linha de performance ao lado da mídia. Perfis verificados e mecanismos de autenticação de voz dependem de processos de homologação e aprovação externa. Deixar essas decisões para novembro, portanto, pode significar chegar atrasado justamente ao período de maior exposição.

Também é necessário concentrar o volume da campanha nos canais verificados, medindo o impacto dessa estratégia, comparando indicadores como entrega, leitura, resposta e conversão, além de acompanhar tentativas de uso indevido da marca. Essa lógica não deve terminar com a venda, já que confirmações de compra, informações de rastreio e atendimento precisam seguir, sempre que possível, pelos mesmos canais reconhecidos pelo consumidor.

A Black Friday, portanto, é mais do que um período de alta nas vendas: é o teste de estresse anual da confiança na comunicação digital das marcas. Nesse cenário, a indústria de mensageria tem a responsabilidade em tornar a verificação um padrão, e não uma escolha opcional.

Para as empresas, isso significa antecipar homologações, concentrar a comunicação em canais autenticados, medir o impacto sobre a performance e manter a identidade consistente durante toda a jornada. Aquelas que chegarem verificadas à Black Friday, certamente converterão melhor na temporada e sairão dela com uma base que, verdadeiramente, reconhece e responde aos seus canais o ano todo.



gesrey_CANVA

(*) Diretor de Growth Platforms da Pontaltech, empresa especializada em soluções integradas de VoiceBot, SMS, e-mail, chatbot, WhatsApp e RCS.