Empresas & Negócios

Matéria de capa

123ducu_CANVA

DESAFIO

FRAUDES EM TRANSPORTES MINAM A SEGURANÇA: O QUE AS EMPRESAS PRECISAM FAZER?

As fraudes no setor de transportes representam um desafio significativo para a segurança de empresas e consumidores. No setor de aplicativos de transporte, as fraudes são um problema crescente. Um relatório da Juniper Research estima que os golpes devem gerar prejuízos de US$ 48 bilhões até 2027. Isso inclui golpes como perfis falsos, phishing e fraudes de pagamento, que afetam diretamente a confiança dos usuários nessas plataformas.

Thiago Bertacchini (*)

Esses dados alarmantes mostram com clareza que empresas precisam adotar medidas robustas de segurança, tanto em estratégia quanto em conscientização, para mitigar os riscos e proteger seus clientes.

Fraudes comuns no setor de transporte - Golpes que exploram plataformas digitais de transporte têm se tornado cada vez mais sofisticados. Entre as fraudes mais comuns, destacam-se:

Golpes das falhas de pagamento – Passageiros fraudulentos podem simular problemas técnicos no celular ou aplicativos de banco para evitar o pagamento da corrida. Essa tática tem como objetivo fazer com que o motorista não receba pelo serviço prestado, prejudicando financeiramente os condutores.

Phishing – Em alguns casos, golpistas se passam por motoristas ou passageiros e enviam links fraudulentos, solicitando que os usuários preencham informações pessoais ou bancárias. Uma vez que os dados são inseridos nesses links, eles são utilizados de forma indevida, gerando prejuízos para as vítimas.

Por isso, é crucial que a plataforma de transporte verifique a veracidade das informações dos motoristas, especialmente com ferramentas que permitam que essa verificação seja escalável e em tempo real, como com uso de inteligência artificial.

Perfis falsos – Golpistas criam contas em plataformas de transporte que, muitas vezes, foram registradas recentemente e não possuem avaliações. Essas contas fraudulentas tendem a oferecer preços atrativos para atrair passageiros desavisados e, em seguida, tentam obter pagamentos fora das plataformas seguras.

No transporte aéreo, as fraudes também são uma preocupação constante. Devido à natureza digital das transações, fraudes como a utilização de cartões de crédito roubados para a compra de passagens são frequentes. Esses "pagamentos" fraudulentos podem ser difíceis de detectar, pois muitas vezes ocorrem em endereços IP diferentes do habitual do cliente, prática já considerada como suspeita.

Para mitigar os riscos, empresas devem investir em medidas de segurança proativas como:

123ducu_CANVA

Biometria comportamental – Essa tecnologia analisa o comportamento do usuário durante a interação com o dispositivo, como padrões de digitação, movimentos do mouse e até o estilo de navegação na internet, com o intuito de verificar a identidade de forma contínua e sem interferir na experiência do usuário.

Segmentação de público – Algumas plataformas oferecem funcionalidades específicas para determinados grupos. Essa segmentação reduz o risco de golpes e incidentes de segurança, criando um ambiente mais controlado e confiável para passageiros e motoristas.

Impressão digital de dispositivos – Uso de uma solução sofisticada de detecção de fraudes para aumentar a segurança, identificando e monitorando dispositivos que tentam acessar uma plataforma. Ajuda a identificar e reduzir comportamentos maliciosos de bots e agentes maliciosos, bem como sinalizar comportamentos suspeitos de dispositivos.

Monitoramento constante de transações – No caso do transporte aéreo, o monitoramento contínuo das transações é essencial. Implementar sistemas de análise de comportamento que detectem atividades suspeitas em tempo real pode ajudar a bloquear fraudes antes que causem danos financeiros, reduzindo significativamente o prejuízo causado pelos fraudadores.

Educação e conscientização – Além de usar tecnologia a favor da segurança, a conscientização dos usuários é uma medida fundamental. Empresas devem educar motoristas e passageiros sobre as práticas recomendadas, como evitar pagamentos fora das plataformas e desconfiar de links enviados por mensageiros externos.

Autenticação de dois fatores (2FA) – Essa tática adiciona uma camada extra de segurança ao exigir que os usuários confirmem sua identidade por meio de um segundo dispositivo ou método de autenticação. Isso ajuda a prevenir acessos indevidos e reduz as chances de ataques cibernéticos, como phishing e roubo de credenciais.

Ao aumentar a segurança da plataforma, a empresa fortalece sua reputação e conquista a confiança dos consumidores. Com uma base de usuários confiantes, é possível aumentar a fidelidade e, consequentemente, a retenção de clientes. Além disso, a prevenção de fraudes reduz custos operacionais relacionados a disputas financeiras e reembolsos. Empresas que não implementam estratégias eficazes de proteção acabam enfrentando prejuízos financeiros significativos, não apenas pelos valores roubados, mas também pela perda de credibilidade no mercado.

O impacto positivo também se reflete na diminuição do churn, ou seja, na retenção de clientes que se sentem seguros ao utilizar os serviços da empresa. Plataformas que não priorizam a segurança tendem a perder usuários para concorrentes que oferecem maior proteção, impactando diretamente suas receitas.

Por outro lado, a negligência na adoção dessas medidas pode resultar em graves consequências. Empresas que não investem em tecnologias de ponta para segurança correm o risco de enfrentar uma onda crescente de fraudes, além de sofrerem penalidades regulatórias, dependendo da gravidade dos casos.

Isso sem mencionar a possibilidade de litígios movidos por consumidores que se sintam prejudicados. Ao compreender a importância de proteger suas operações e clientes contra fraudes, as empresas estarão mais bem posicionadas para enfrentar os desafios desse cenário digital em evolução.

(*) - É Head de Vendas da Mangopay (https://mangopay.com/).