Digitalize + Prospere

PROTEJA SUA EMPRESA CONTRA FRAUDES

Como se manter na dianteira na corrida pela cibersegurança

PayPal

O QUE É A ECONOMIA DAS FRAUDES?

Costumávamos pensar em fraude on-line como incidentes isolados conduzidos por hackers e golpistas individuais. Mas, nos últimos anos, esses tipos de crimes cibernéticos passaram a ser cometidos cada vez mais por quadrilhas coordenadas e sofisticadas. Para se protegerem contra fraudes, as empresas devem implementar proteções igualmente sofisticadas.

A pandemia mudou todas as regras do jogo, especialmente no comércio eletrônico. O início da COVID-19 gerou um aumento de 60% no tráfego on-line e, como resultado, os gastos em compras globais quase dobraram[1]. Em 2021, as ameaças de fraude foram piores do que nunca. Os varejistas de comércio eletrônico correram o risco de perder mais de US$ 20 bilhões devido a atividades online fraudulentas. Isso representou um aumento de 18% nas atividades fraudulentas em comparação com o ano anterior[1]. Em meio ao cenário estressante da pandemia, os fraudadores fingiram ser instituições de caridade, mandaram e-mails se passando pela Organização Mundial da Saúde (OMS) ou pelo Centro de Controle e Prevenção de Doenças dos EUA (CDC) e até mesmo fizeram ligações automáticas fingindo ser organizações governamentais, familiares em dificuldades ou bancos e empresas de cartão de crédito[2].

À medida que a economia das fraudes cresce, a audácia dos cibercriminosos aumenta. Eles estão ficando mais inteligentes, mais sofisticados e agora têm maior acesso às ferramentas necessárias para atacar empresas on-line. Eles têm tanto conhecimento (ou mais!) sobre o funcionamento do comércio eletrônico quanto as empresas atacadas. Isso permite que eles identifiquem precisamente as vulnerabilidades de segurança e usem o elemento surpresa para explorá-las[3].

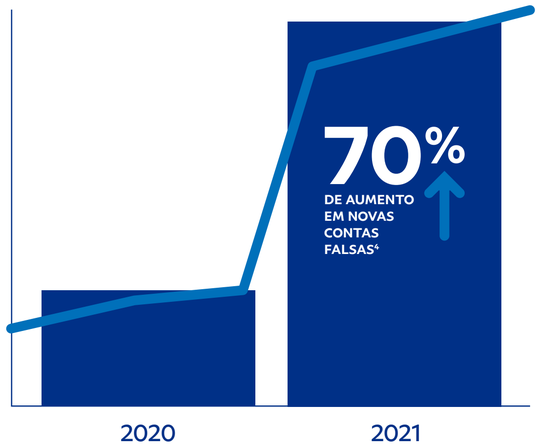
Com o crescimento desenfreado das fraudes, as empresas estão se esforçando como nunca para não ficarem para trás, mas isso não significa que as expectativas dos clientes mudaram. Os compradores on-line ainda esperam uma experiência rápida e descomplicada, além de segurança impenetrável. Se as compras demoram muito, exigem muitos dados ou são muito complexas, os clientes abandonam seus carrinhos e buscam outra empresa. Essas expectativas são um desafio para os vendedores que buscam atender às demandas dos consumidores e, ao mesmo tempo, se proteger contra várias ameaças cibernéticas.

1. Payments Dive, E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds, 30 de abril de 2021. **2.** CyberCrime Support Network, COVID-19 Scam Alerts, 12 de abril de 2021. **3.** Sift, Exposing the Multi-billion Dollar Fraud Economy, 1º trimestre de 2021.

AS EMPRESAS ENFRENTAM NOVOS DESAFIOS COM AS FRAUDES MUNDO AFORA

AUMENTO EM FRAUDES DE NOVAS CONTAS

Em 2021, o registro de novas contas falsas aumentou em mais de **70%**[4].



MOVIMENTOS OUSADOS VISANDO ALVOS MAIORES

Cada compra fraudulenta tem um valor médio **70%** maior do que a média antes da pandemia[5].

O CRESCIMENTO DOS ATAQUES MÓVEIS

50% de todo o tráfego digital foi em dispositivos móveis e a taxa de ataques móveis foi de **24%** na primeira metade de 2021[6].

4. Business Wire, 70% Increase in Fraudulent Account Registrations Puts Digital Accounts in the Crosshairs, Arkose Labs Reports, 5 de agosto de 2021. **5.** Retail Week, Every day is now Black Friday – and retailers need to prepare, 4 de novembro de 2021. **6.** Security Boulevard, Here's How to Fight Diverse Attacks Across Multiple Touchpoints, 8 de outubro de 2021.

MANTENHA-SE UM PASSO À FRENTE DOS CIBERCRIMINOSOS

Já que as ameaças cibernéticas estão mais complexas e difundidas do que nunca, as empresas não podem mais simplesmente considerar que as fraudes fazem parte dos custos operacionais. No ano passado, o varejo multicanal observou um aumento de 50% ano a ano nas fraudes e um aumento de 9% ano a ano no volume dos pedidos fraudulentos[7]. Por isso, as empresas devem focar em adotar a infraestrutura adequada para se proteger contra fraudes.

5 dicas para proteger sua empresa:

1. Monitore seu site contra atividades suspeitas
2. Bloqueie os crimes cibernéticos no checkout
3. Criptografe seus dados para proteger os pagamentos
4. Atualize seu software para aprimorar sua segurança
5. Identifique seus pontos fracos para aumentar sua segurança on-line

7. Sift, Exposing the Multi-billion Dollar Fraud Economy, 1º trimestre de 2021.

1 MONITORE SEU SITE CONTRA ATIVIDADES SUSPEITAS

Atividades suspeitas podem custar tempo e dinheiro à sua empresa, mas nem sempre são fáceis de detectar. Vale a pena estar vigilante, então listamos algumas maneiras de ficar de olho em seu site.

Desconfie de estornos excessivos. Reclamações de estorno de compras desconhecidas ou esquecidas e um não entendimento das políticas de devolução podem indicar fraude de estorno (também conhecida como fraude amigável ou fraude primária). A fraude amigável é apontada por 94% das empresas como um problema[8].

Você pode identificar sinais de atividade incomum de consumidores, ficando atento a endereços em um mercado desconhecido e prestando atenção aos casos em que os endereços de cobrança e envio não coincidem. Além disso, tenha cuidado com endereços de e-mail suspeitos, e-mails não entregues, pedidos inusitadamente grandes ou pagamento de um pedido com vários cartões de crédito.

Mesmo quando você presta mais atenção à atividade do seu site, recorrer aos especialistas é sempre uma boa ideia. Se for possível, terceirize a gestão de estornos para um provedor especializado, para aliviar você e sua equipe do fardo de monitorar esses padrões. Também existem ferramentas que rastreiam os endereços IP dos clientes e alertam quando eles estão em locais de alto risco.

Os recursos de prevenção de fraude e proteção ao vendedor da PayPal Commerce Platform podem ajudar, utilizando aprendizado de máquina que se adapta às necessidades da sua empresa para minimizar estornos e oferecendo cobertura contra certas atividades fraudulentas.

8. Business Wire, 8 Out of 10 Merchants Have Seen an Increase in Friendly Fraud, According to the 2021 Chargebacks911 Field Report, 2 de junho de 2021.

2 BLOQUEIE OS CRIMES CIBERNÉTICOS NO CHECKOUT

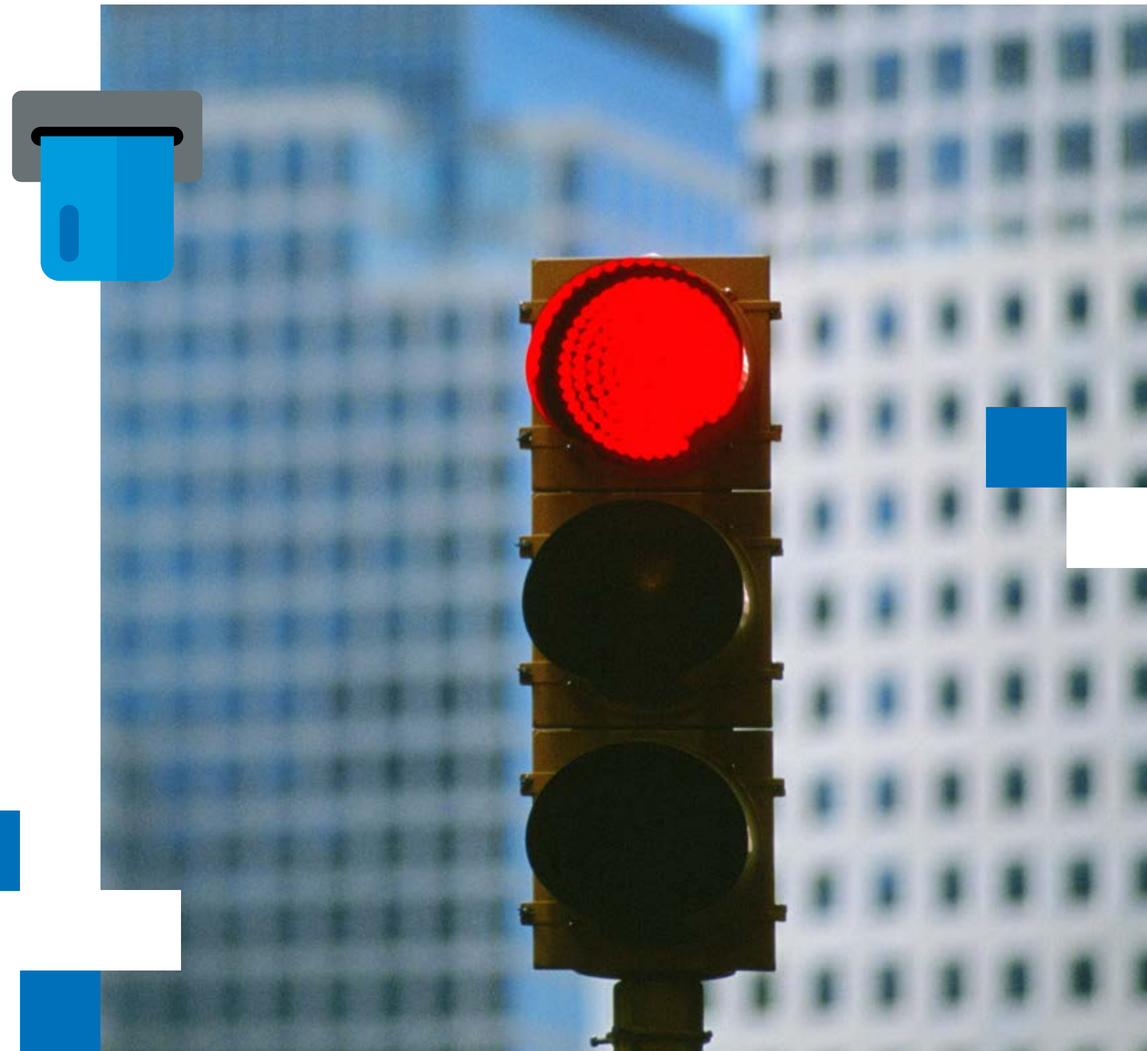
59% das empresas observaram um aumento nas fraudes de transações com cartão ausente, mas soluções de proteção contra fraude no checkout podem ajudar você a se antecipar a esses tipos de ataques[9].

1 em cada 4 comerciantes tem dificuldades para implementar soluções de segurança de pagamento, mas seguir essas etapas é essencial para empresas que começam a se expandir para o comércio eletrônico[9].

Exigir os códigos de verificação de cartão (CVV) praticamente impossibilita que os cibercriminosos cometam fraudes de cartão ausente, já que as regras PCI impedem que os vendedores armazenem o CVV com o número do cartão de crédito. Isso garante que o cliente tenha o cartão físico em sua posse ao fazer uma compra[10].

O sistema de verificação de endereço (AVS) ajuda a identificar atividades suspeitas, comparando as partes numéricas do endereço de cobrança associado ao cartão de crédito com o endereço registrado na administradora do cartão de crédito. O AVS também está incluído na maioria dos sistemas de processamento de pagamentos, mas é uma boa ideia verificar com seu processador de pagamentos para ter certeza de que ele é compatível.

Por último, a verificação de velocidade é um mecanismo de prevenção de fraude que permite limitar a quantidade de fundos ou transações provenientes de um cliente em um mesmo dia. Você pode definir qualquer limite que faça sentido para a sua empresa e receber uma notificação quando alguém tentar ultrapassá-lo; o sistema pode até mesmo cancelar a transação automaticamente. Isso geralmente é feito para impedir a ação de fraudadores que tentam usar todo o limite de cartões de crédito roubados.



9. Payments Dive, Merchants say they're losing revenue to online fraud, FIS report finds, 12 de julho de 2021. **10.** Big Commerce, Ecommerce Fraud Protection for Online Merchants: The Ultimate Guide.

3 CRIPTOGRAFE SEUS DADOS PARA PROTEGER OS PAGAMENTOS

Os dados não criptografados são os melhores amigos do cibercriminoso. Eles permitem que os fraudadores tenham facilmente acesso a números de cartão de crédito, senhas e muito mais. Embora observe-se uma mudança em direção a alvos de maior valor, muitos cibercriminosos ainda aproveitam essas oportunidades fáceis.

Uma grande quantidade de dados confidenciais é enviada pela internet todos os dias. A possibilidade de que eles caiam nas mãos erradas é alta, mas existem medidas que você pode adotar para garantir que isso não prejudique sua empresa ou seus clientes.

A criptografia de ponta a ponta prepara você para essas situações, convertendo os dados em código secreto antes de serem enviados pela internet. As leis de privacidade e proteção de dados locais exigem que empresas que armazenem ou compartilhem dados adotem essa tecnologia[11].

Dê um passo além e garanta que suas conexões HTTPS sejam seguras usando configurações fortes de Transport Layer Security (TLS). As configurações de TLS são o padrão atual do setor e permitem que suas informações viajem pela internet com segurança.

Verifique se o seu parceiro de pagamentos leva a segurança dos seus dados tão a sério quanto você e atende aos rigorosos requisitos de proteção de dados.

A plataforma de pagamentos do PayPal conta com algumas das melhores criptografias de ponta a ponta. De conexões TLS e HTTPS à pinagem de chave, nossas práticas estão em conformidade com os requisitos rigorosos que protegem os dados em trânsito e em repouso.

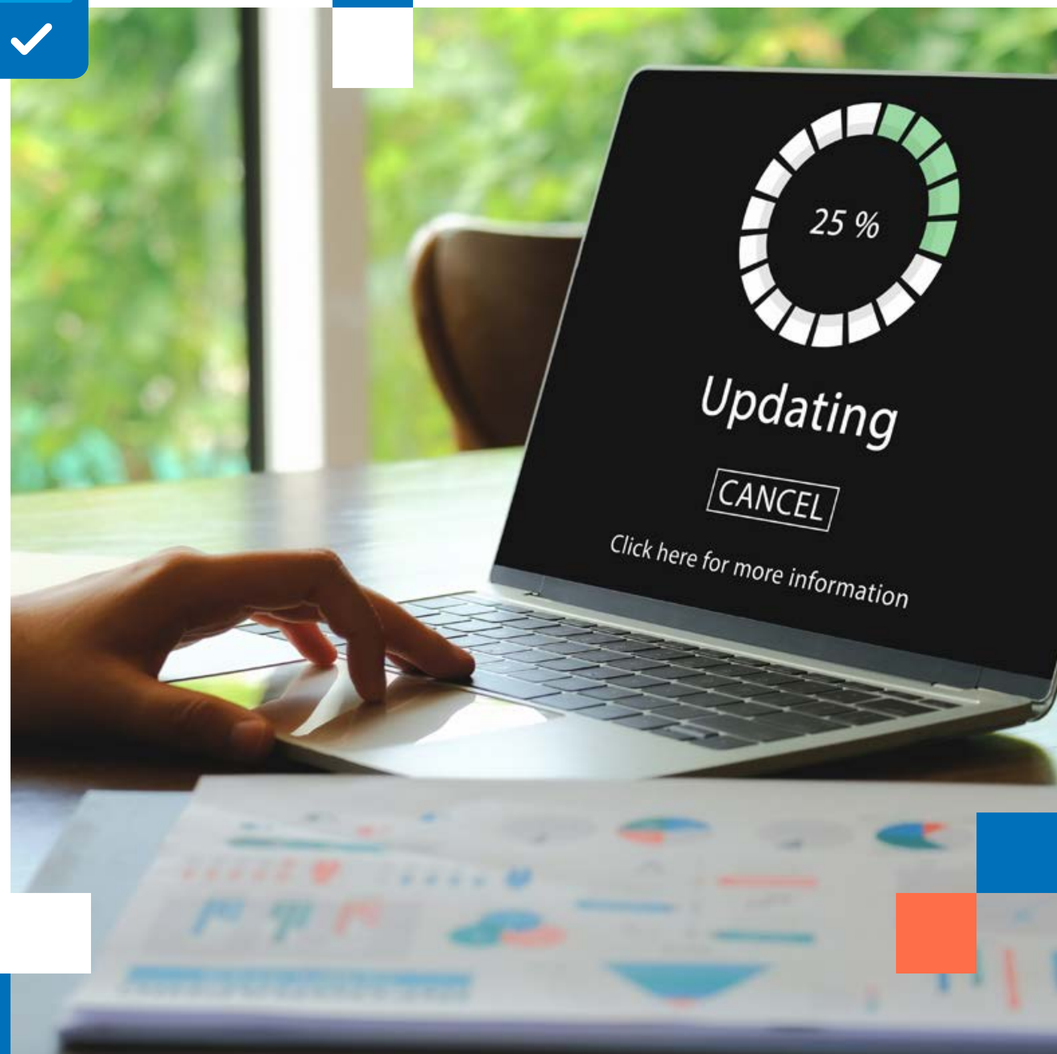
11. Insurance Business Magazine, Ten ways to protect your business from cyber attacks, 20 de março de 2021.

4 ATUALIZE SEU SOFTWARE PARA APRIMORAR SUA SEGURANÇA

Software desatualizado é uma das formas mais fáceis de permitir que os cibercriminosos invadam seus sistemas[12]. Veja algumas medidas que você deve adotar para encerrar esta política de portas abertas que você não sabia que tinha com o crime cibernético.

Embora manter seu sistema operacional (SO) atualizado seja uma maneira simples e eficaz de adicionar uma camada de proteção à sua empresa, 95% dos sites ainda rodam em software desatualizado que apresentam vulnerabilidades conhecidas[13]. Os provedores de sistemas operacionais atualizam continuamente seus sistemas com patches de segurança para se antecipar às ameaças, vírus e malware mais recentes. Mesmo uma pequena atualização do sistema operacional pode ter um grande impacto na segurança da sua empresa[12].

Usar antimalware e antispyware de nível empresarial é outra maneira de evitar ataques que visam vulnerabilidades de software desatualizado – e você deve atualizá-los regularmente[14]. Também é importante destacar que softwares gratuitos para pessoas físicas são insuficientes devido à limitação de funções e cobertura. Eles não atendem às necessidades das empresas e podem acabar custando mais no longo prazo.



12. Business 2 Community, Top 5 Risks of Using Outdated Software in Your Company, 14 de junho de 2021. **13.** Cybernews, 95% of websites run on outdated software with known vulnerabilities, 18 de março de 2021.
14. Business 2 Community, 6 Ways to Keep Your Business Data Safe, 26 de outubro de 2021.

5 IDENTIFIQUE SEUS PONTOS FRACOS PARA AUMENTAR SUA SEGURANÇA ON-LINE

Os cibercriminosos são os ladrões do futuro. Eles sabem como explorar a tecnologia e inovação, mas também visam os momentos de desatenção das vítimas, como um batedor de carteira da velha guarda. Por exemplo, quando o tráfego da internet aumentou nos ambientes de jogos e criptomoedas, os cibercriminosos sabiam que as equipes de risco ficariam muito sobrecarregadas com o aumento do tráfego e não conseguiriam pegar todas as fraudes[15].

Os cibercriminosos usam estratégias sofisticadas para realizar ataques altamente lucrativos. Por isso, é fundamental se informar e preparar sua empresa. Conheça suas vulnerabilidades e, principalmente, não subestime um cibercriminoso.

Um ponto fraco com o qual a maioria das empresas se identifica são as temporadas de compras sazonais de alto tráfego, como Black Friday, Cyber Monday e Dia dos Solteiros. As vendas disparam e as distrações também: os cibercriminosos sabem disso e se aproveitam.

Na outra ponta do espectro, um tráfego excepcionalmente baixo pode ser outra vulnerabilidade. Quando o setor de transporte vivenciou uma queda significativa na demanda devido à COVID-19, os cibercriminosos buscaram contas de clientes inativas para obter pontos de recompensa e dados de pagamento[15].

Implementar as proteções corretas durante os períodos mais movimentados permite que você aproveite seus lucros em paz. Por outro lado, manter a guarda quando o movimento está fraco garante que sua empresa não dê chance aos fraudadores.

15. Sift, Exposing the Multi-billion Dollar Fraud Economy, 1º trimestre de 2021.

FORTALEÇA SUA CIBERSEGURANÇA COM O PAYPAL

O aumento do comércio eletrônico e dos crimes cibernéticos colocou a cibersegurança em uma posição de prioridade em todo o mundo. Com a maior prevalência e sofisticação das fraudes, contar com um parceiro de pagamentos confiável não é mais apenas uma coisa boa – é essencial. A parceria com o PayPal oferece tranquilidade em todas as transações. Nossa rede poderosa processa com segurança mais de 10 milhões de pagamentos por dia e fica mais inteligente a cada transação. Obtenha as ferramentas necessárias para vender com segurança e confiança mundo afora.

Comece já →