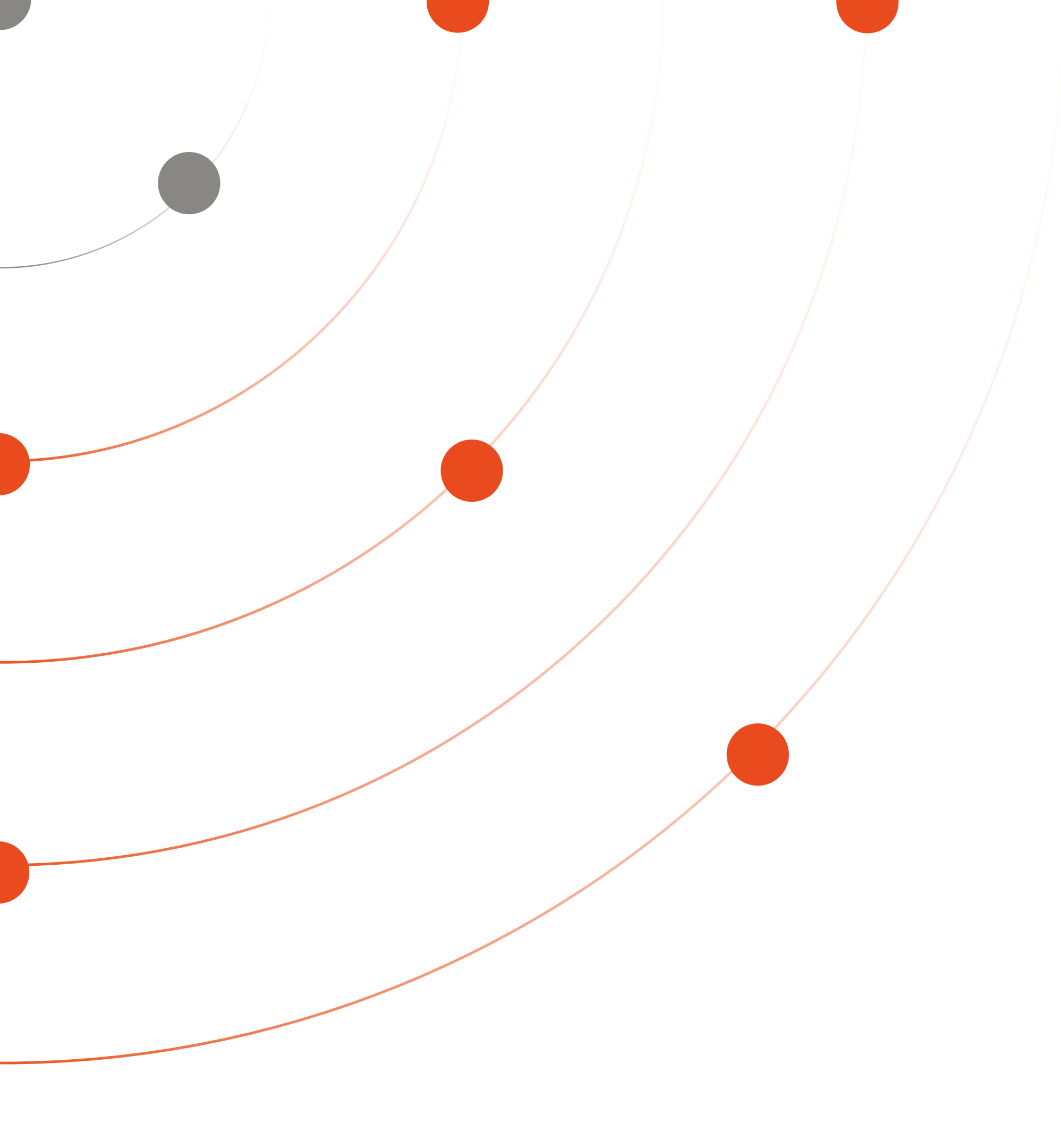




GLOSSÁRIO DAS FRAUDES NO ECOMMERCE: ENTENDA TODOS OS TERMOS



ClearSale



Introdução	3
Por que conhecer os termos de fraude em e-commerce	5
Glossário de termos de fraude no e-commerce	7
Como se proteger	21
Conclusão	24
Sobre a ClearSale	26

INTRODUÇÃO



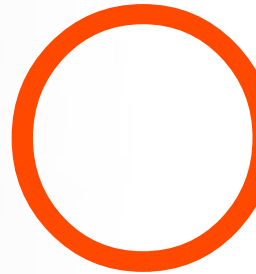
As fraudes tornaram-se recorrentes nos mais diferentes segmentos, especialmente pela criatividade cada vez mais aguçada dos fraudadores. Isso ocorre, sobretudo, devido a algumas **fragilidades associadas à compra por meio do comércio eletrônico**.

Neste e-book, apresentaremos um glossário com alguns dos principais termos utilizados para identificar os diferentes tipos de fraudes no e-commerce, bem como as soluções e as **formas de prevenção**. Saiba quais são e como se proteger!

POR QUE CONHECER OS TERMOS DE FRAUDE EM E-COMMERCE

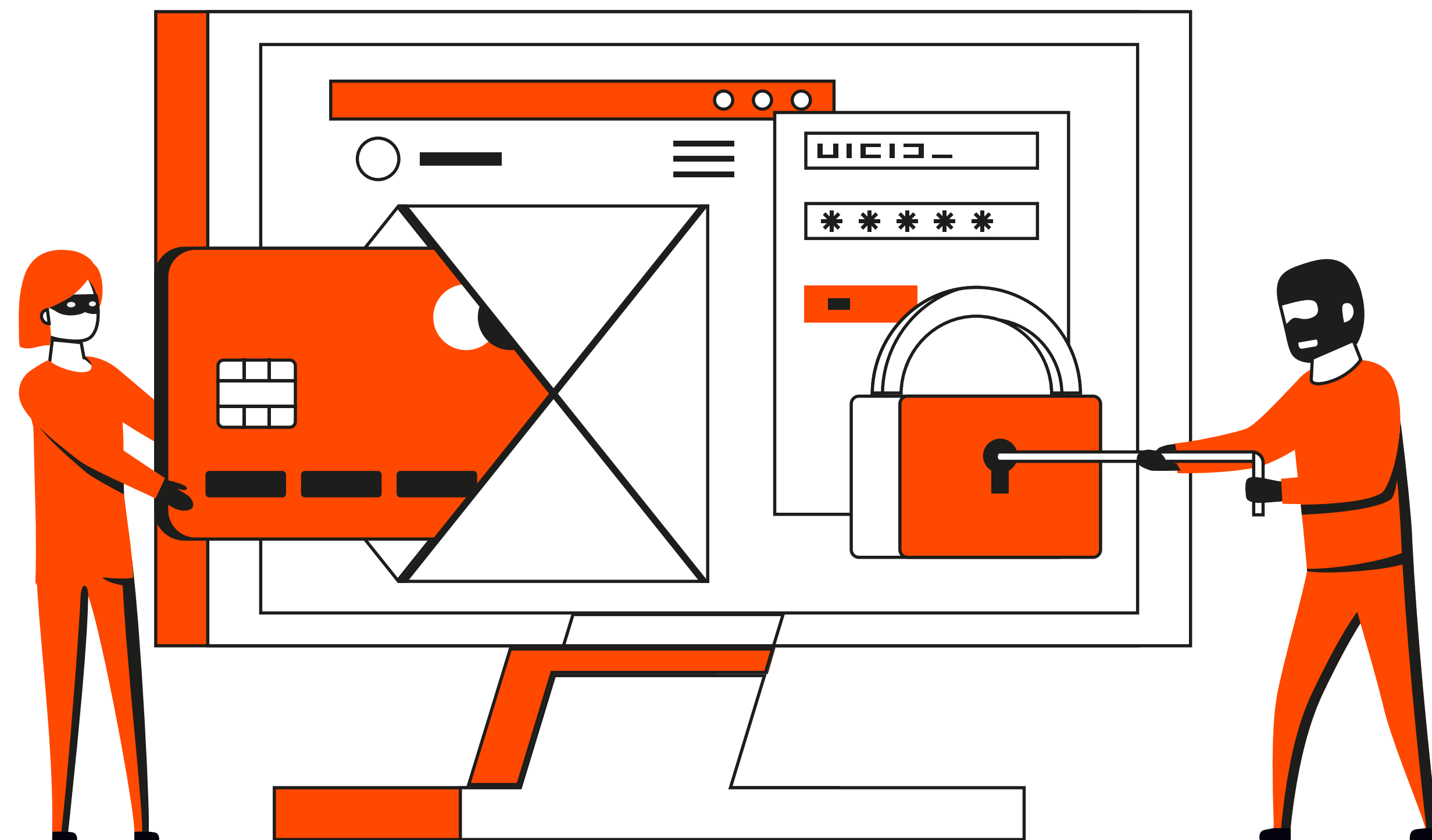




 universo das fraudes vai muito além de uma pessoa cometendo **crimes cibernéticos**. Elas **podem provocar graves danos** à vítima, tanto financeiros quanto psicológicos ou, até mesmo, de imagem ao varejista.

Por ser bastante complexa e prejudicar os negócios e seus clientes, é importante conhecer os termos utilizados nas diversas situações que podem levar a ocorrências de fraude, bem como os termos relacionados às soluções que podem garantir uma boa prevenção.

GLOSSÁRIO DE TERMOS DE FRAUDE NO E-COMMERCE



A quantidade de **denominações para classificar crimes eletrônicos** é equivalente aos crimes praticados e, assim como esses, cresce a cada dia. Conheça, a seguir, alguns dos principais termos utilizados para identificar fraudes no comércio eletrônico e aqueles adotados para nomear soluções visando ao combate e à prevenção.

Agência de crédito

São agências que coletam e vendem dados relacionados à qualidade de crédito de uma pessoa. Elas coletam informações valiosas que permitem aos credores decidirem **o quanto confiável é um indivíduo no pagamento de suas dívidas**. Pelo fato de lidarem com informações confidenciais, tornam-se particularmente suscetíveis a ataques cibernéticos e violações.

Arbitragem

A arbitragem acontece quando uma **terceira pessoa, imparcial, resolve uma disputa entre duas partes fora do litígio**, ouvindo suas evidências e testemunhos para tomar uma decisão. O e-commerce utiliza cada vez mais a resolução de disputas online para solucionar problemas com uma transação.



Assinatura digital

A assinatura digital auxilia na **conferência da autenticidade de uma mensagem ou documento digital**. Ela proporciona confiabilidade à origem dos dados e garante que eles não sofreram alterações durante o trânsito. Trata-se de autenticações criptografadas, equivalentes às assinaturas legais manuscritas em diversos países.

Autenticador

Os serviços proporcionados por um autenticador oferecem uma **camada extra de proteção aos clientes**. Isso porque eles confirmam a identidade de um cliente durante o processo de login ou checkout em uma página de e-commerce e no momento do pagamento.

Isso pode ser feito por meio de perguntas que somente a pessoa sabe a **resposta ou por biometria**. Embora esse sistema possa provocar atrito à experiência do cliente, evita que as contas dos usuários sejam comprometidas.

Autofraude

Enquanto os demais tipos de fraudes no comércio eletrônico são provocados por terceiros, essa é uma **ação realizada pelo próprio titular do cartão**. Para isso, ele realiza a compra online e, no prazo concedido pela instituição financeira (180 dias), contesta a transação, alegando que não fez a compra, mesmo já tendo recebido o produto ou serviço.

Autorização

A solicitação de autorização para o valor a ser transacionado é enviada do lojista para o banco adquirente. Em seguida, vai para o banco emissor do cartão. Caso seja aprovada, o valor da compra é deduzido da conta do titular do cartão e ele recebe uma confirmação da compra.



AVS

O sistema de verificação de endereço (AVS) é um **filtro de fraude** que diversos comércios eletrônicos usam para bloquear pedidos potencialmente fraudulentos. Para a transação ser aprovada, as partes numéricas dos endereços de cobrança e remessa que um cliente insere devem corresponder às registradas no banco emissor do cartão. Caso contrário, a transação pode ser recusada ou sinalizada para revisão manual.



Botnet

Esse termo é uma combinação das palavras “robô” (bot) e “rede” (net). Em geral, se refere a uma **sequência maliciosa de dispositivos conectados à internet**, utilizados para roubar dados e comprometer outros computadores e sistemas.

Big Data

Refere-se ao **volume de informações que uma empresa coleta e armazena diariamente de diversas fontes**, como dados de clientes, transações comerciais, correspondência por e-mail, bem como presença nas mídias sociais. O e-commerce pode utilizar esses dados para obter informações detalhadas sobre **o comportamento do consumidor e identificar tendências de negócios**.

CVC

As compras online geralmente solicitam o número do **Código de Verificação do Cartão de Crédito** (CVC) como forma de os varejistas de comércio eletrônico verificarem se o consumidor possui, de fato, o cartão utilizado na compra. São três ou quatro dígitos impressos (sem relevo) no verso do cartão.

Embora essa identificação não seja necessária para as transações online, fornece uma **camada extra de segurança** para o titular do cartão, assim como para o comerciante.

Chargeback

O **chargeback**, que em tradução livre significa **estorno**, ocorre quando o titular do cartão identifica uma **transação questionável no extrato do cartão de crédito** e reclama junto ao emissor do cartão de crédito.

Se o emissor entender que o titular do cartão não efetuou a compra e, portanto, a transação foi efetuada com um cartão roubado, ou se o produto não foi recebido, o valor da transação é reembolsado, sendo cobrada uma taxa adicional do comerciante.





Comerciante multicanal

Os comerciantes multicanais têm o foco voltado em colocar seus produtos nas mãos dos clientes, onde quer que estejam por meio de **sites e redes sociais**. São canais diversificados que extrapolam a venda física, por telefone e catálogo.

Criptografia

A **criptografia** é uma tecnologia que **codifica dados** para que apenas as partes autorizadas possam acessá-los. As informações criptografadas dificultam o acesso impedindo a interceptação para fins ilegais. Mesmo que elas sejam interceptadas por um hacker, ele não conseguirá decodificá-las sem a chave de descryptografia.

Engenharia Social

Essa é uma das maiores **ameaças de segurança** que as empresas enfrentam atualmente. A **Engenharia Social engana as pessoas**, por meio de um conjunto de ações, para que violem a segurança e divulguem informações ou executem alguma ação nesse sentido.

Para isso, os fraudadores se apresentam como autoridades ou representantes de empresas para obter dados confidenciais, por meio de métodos não técnicos, como o phishing.

Falsas recusas

As **falsas recusas** (ou **falsos positivos**, como também são chamadas) ocorrem quando uma transação legítima é sinalizada pelo sistema de proteção contra fraudes e recusada. Em geral, isso pode acontecer quando o titular do cartão solicita o envio dos produtos comprados para endereço diferente do cadastrado. Com isso, o cliente é identificado erroneamente como fraudador e não consegue finalizar a compra.

Filtros de velocidade

Os **filtros de velocidade** monitoram elementos de dados **específicos** (como endereço de e-mail, número de telefone e endereços de cobrança/envio). Eles limitam o número de transações que um site pode processar em um determinado período (uma hora, um dia). Isso evita que um fraudador tenha tempo para testar diversos números de cartões roubados, a fim de verificar se funcionam.





Fraude amigável

A **fraude amigável** acontece quando o titular de cartão contesta uma compra ou solicita estorno porque simplesmente não sabe que alguém próximo, como um amigo ou familiar, usou o cartão para realizar a transação. O que diferencia esse de outros tipos de fraude é que, nessas situações, **não há intenção** de enganar uma vítima ou obter algum tipo de ganho com a situação.

Fraude de cartão de crédito

Esse tipo de fraude inclui **roubo ou suposição de identidade**. Os fraudadores podem acessar os dados do cartão de crédito de uma vítima por meio da compra de informações na deep web ou dark web (parte oculta da web), usando skimmers (leitores de cartão) em bombas de postos de gasolina ou por meio de violações dos dados corporativos, além de outros métodos.

Fraude de pagamento

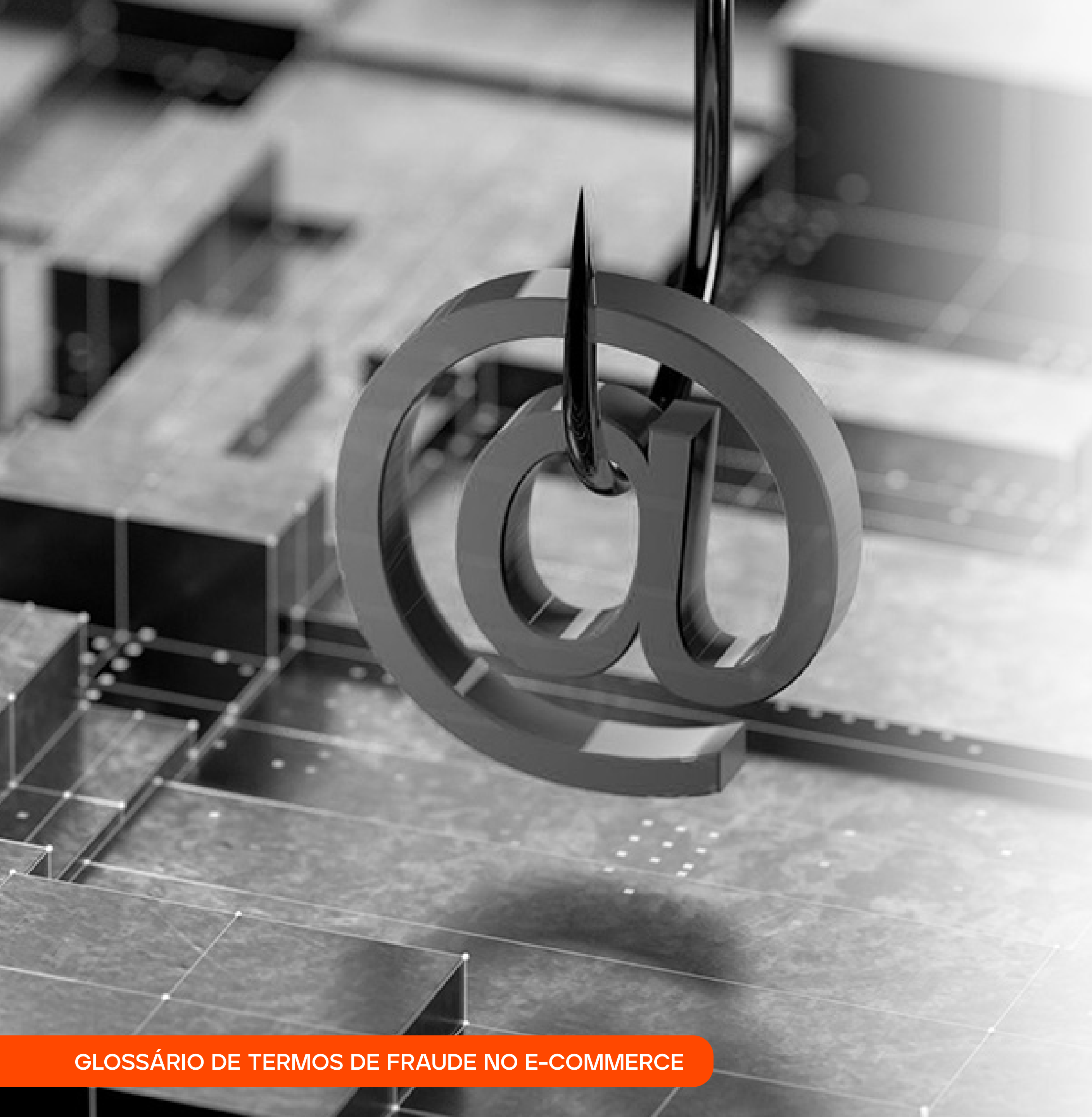
Refere-se a **qualquer transação fraudulenta** executada por um criminoso que resulte no roubo de dinheiro, propriedade ou acesso às informações confidenciais da vítima. Os fraudadores se envolvem cada vez mais em comportamentos sutis para enganar consumidores desavisados que liberam dados pessoais.

Fraude de estorno

Embora os estornos existam para proteger os consumidores contra as perdas por roubo de identidade e práticas comerciais desleais envolvendo cartões de crédito, alguns **clientes mal-intencionados registram um estorno indevido em uma transação legítima**. Assim, eles ficam com o produto e recebem um reembolso total da compra.

Malware

Esse termo é uma abreviação de “software malicioso”, **projetado para danificar computadores, servidores e até redes por meio de vírus de computador**, como ransomware, spyware e outros. Quando instalado no computador da vítima, pode capturar inclusive as teclas digitadas pelo usuário enquanto ele insere nomes de usuário, senhas e e-mails. Com isso, os fraudadores conseguem acessar as contas e utilizar os saldos para compras fraudulentas.



Phishing

Também chamado **pesca de dados**, essa é uma forma muito difundida de Engenharia Social. Trata-se de roubo de identidade e uma das ocorrências fraudulentas que mais crescem no ambiente online. Acontece quando o criminoso envia e-mail ou mensagem de texto com um link falso.

Ao acessá-lo, **o navegador é redirecionado para páginas alteradas, contendo vírus maliciosos que se instalam na máquina da vítima**. A partir daí, ela corre o risco de exposição de seus dados pessoais, que podem gerar transações comerciais indevidas.

Proteção de estorno

Normalmente, a **proteção de estorno cobre uma parte das perdas** que uma empresa pode sofrer devido a transações fraudulentas. Contudo, ela não reembolsa totalmente os comerciantes. Em vez disso, eles podem receber descontos na fatura com base em KPIs pré-determinados.

Roubo de dados em sites falsos

Muitos fraudadores utilizam a tecnologia para tirar vantagem de pessoas, inclusive criando sites idênticos aos das lojas de interesse do consumidor, com locais de cadastramento para **roubar os dados sensíveis**. A partir disso, utilizam as informações de maneira indevida em vários tipos de fraudes, em benefício próprio.

Tokenização

Os **serviços de pagamento como Apple e Android utilizam a tokenização** para proteger os dados confidenciais, trocando as informações pessoais por dados gerados aleatoriamente. Dessa forma, os dados reais do cartão de crédito de uma pessoa nunca são acessados ou usados.

Esse é um processo sem atrito e quase invisível para os consumidores. Além disso, ajuda a proteger contra o roubo de dados do cartão de crédito durante uma transação e auxilia os comerciantes a cumprir os padrões de segurança do setor, como o PCI DSS.



Uso da identidade de outra pessoa

O roubo de identidade é um dos crimes mais praticados há muitos anos. O criminoso se passa por outra pessoa e usa dados da identidade de terceiros para fazer compras em nome da vítima. Em geral, esses dados são obtidos por meio eletrônico, e o **proprietário do cartão não reconhece a compra**, solicitando o reembolso para a operadora do cartão.

COMO SE PROTEGER



Conheça algumas das principais maneiras de se proteger da ação dos fraudadores e oferecer mais segurança aos seus clientes.

Monitore indicadores corretos

A efetividade de uma ação contra a fraude deve ser medida com os indicadores corretos. No caso do e-commerce, por exemplo, **o tempo de resposta, a taxa de aprovação e o chargeback precisam estar em equilíbrio**. Quando um desses não é bom, significa que o combate a fraudes está pouco efetivo.

Utilize sistemas de automação financeira

Os sistemas tecnológicos utilizados em bancos colaboram com a automação financeira e na prevenção de fraudes, especialmente os que facilitam a **conciliação financeira**. Isso porque eles ajudam a reduzir a quantidade de chargebacks e integram todos os pagamentos recebidos por meio de operadoras, viabilizando uma análise completa dos pagamentos.

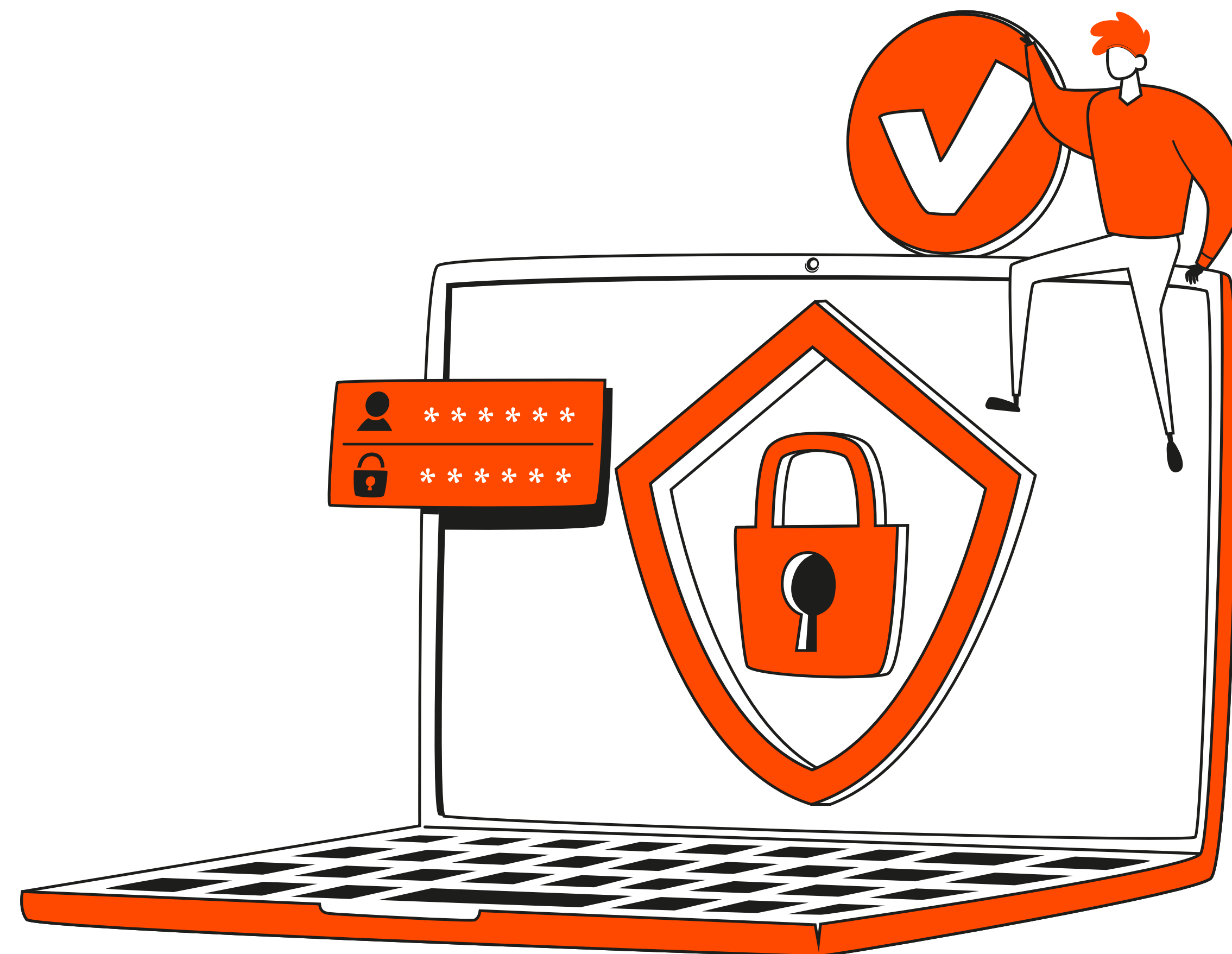
Invista em um sistema antifraude

Diante da quantidade de recursos eletrônicos que os fraudadores contam para atingir as vítimas, não há como combatê-los sem contar com um sistema antifraude robusto. Dessa forma, a melhor atitude a ser tomada é identificar os pontos vulneráveis do negócio e adotar medidas de proteção e prevenção por meio de uma solução especializada.

Nesse sentido, as soluções da ClearSale vão muito além do **combate a fraudes**. Elas ajudam a criar e rastrear os indicadores que auxiliam as empresas no processo de expansão do seu comércio eletrônico. A nossa abordagem exclusiva para prevenir fraudes não se limita a impedir que elas ocorram. Além disso, aprovamos mais pedidos legítimos, o que é fundamental para aumentar as suas vendas.

Isso é possível porque combinamos a tecnologia da inteligência estatística e artificial com uma estrutura altamente eficiente, composta por analistas especializados em fraudes para oferecer uma abordagem equilibrada e diferenciada.

CONCLUSÃO





Conforme mostramos ao longo deste e-book, há vários termos utilizados em fraudes no comércio eletrônico, assim como em seus sistemas de proteção. Nesse sentido, é importante conhecer e entender o significado de cada um para saber identificá-los e saber o que buscar para **proteger o seu comércio eletrônico**.



A ClearSale é especialista em soluções de prevenção e gerenciamento de risco nos mais diversos segmentos, como e-commerce, mercado financeiro, vendas diretas e telecomunicações. A empresa possui um poderoso banco de dados com conhecimento de 97% dos consumidores no mercado digital.

Com capital aberto desde 2021, a ClearSale tem a missão de equilibrar tecnologia e profissionais especializados para entregar excelentes indicadores aos clientes, a fim de gerar cada vez mais confiança no mercado.