evertec

COMO EVITAR QUE SEU NEGÓCIO SEJA VÍTIMA DE FRAUDE

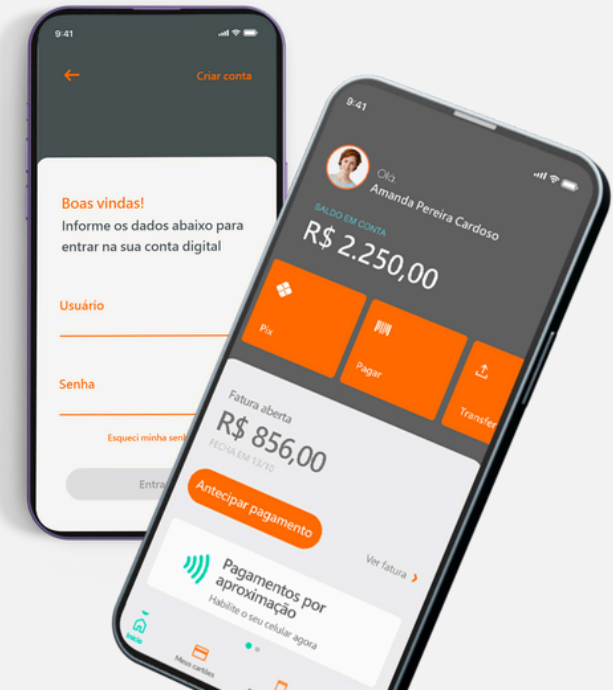
Guia completo para proteger sua empresa contra ameaças cibernéticas

A Evertec (NYSE: EVTC) é uma empresa líder em processamento de pagamentos na América Latina e Caribe. Processamos mais de seis bilhões de transações de pagamentos, anualmente, e fornecemos tecnologia financeira que impulsiona negócios por meio de soluções escaláveis e seguras.

CONTE COM QUEM CONHECE O MERCADO

6 BILHÕES
de transações anuais

26 PAÍSES
com clientes



INTRODUÇÃO

À medida que as tecnologias avançam e surgem novas formas de facilitar compras e transações online, também aparecem novas modalidades de roubo e fraude que visam afetar usuários e proprietários de comércios físicos ou virtuais. Esses atos buscam explorar a ingenuidade dos cibernautas para solicitar seus dados pessoais ou financeiros e roubá-los, ou a seus associados.

Existem várias modalidades e tendências de fraude que evoluem com as tecnologias e dispositivos. À medida que se aperfeiçoam, o número de vítimas aumenta. Portanto, é muito importante que todos os usuários adotem medidas de prevenção e que lojas e comércios online ofereçam plataformas seguras para seus clientes.

Nesse sentido, todos os envolvidos (lojas, consumidores, marcas de cartões, bancos emissores) devem adotar medidas de segurança e estar atualizados com os protocolos e requisitos para oferecer um serviço transparente e eficaz.

Aqui, você conhecerá os tipos de fraudes mais comuns e como evitar que seu negócio se torne vítima deles, protegendo seus ganhos e a segurança de seus clientes.

TIPOS DE FRAUDE

Ao realizar transações na internet, existem vários tipos de fraude. Os **3 mais** comuns são a estafa, o roubo de identidade e a invasão de conta.

1. Estelionato

O estelionato é um delito que causa prejuízo patrimonial a alguém por meio de engano, com intenção de lucro. No caso do estelionato online, o golpista engana e obtém benefícios ao roubar informações financeiras de outras pessoas (por exemplo, vendendo essas informações e lucrando com isso, ou prometendo um produto e não entregando).

Casos de estelionato online mais comuns são:

- **Doações a instituições de caridade ou organizações falsas:** através de redes sociais ou perfis em páginas de crowdfunding.
- **Enganos sentimentais:** através de aplicativos de namoro ou perfis falsos, buscam estabelecer uma relação com a vítima para solicitar dados ou dinheiro.

- **Ofertas falsas de emprego:** costumam oferecer uma posição muito bem remunerada sem exigir experiência, e o remetente do e-mail costuma ser desconhecido e suspeito.

- **Oportunidades de negócio:** oferecem a oportunidade de investir em um negócio, franquia ou produto para ganhar dinheiro rapidamente.

- **Vírus falso:** um banner avisa sobre um falso vírus e leva a uma página para baixar um software que promete eliminar esse vírus do seu computador.

No Brasil, 62% das pessoas estão dispostas a pagar mais por produtos de empresas que garantem segurança online e reduzem o risco de fraudes. Além disso, 86% preferem comprar de marcas que consideram seguras.

Fonte: Serasa Experian

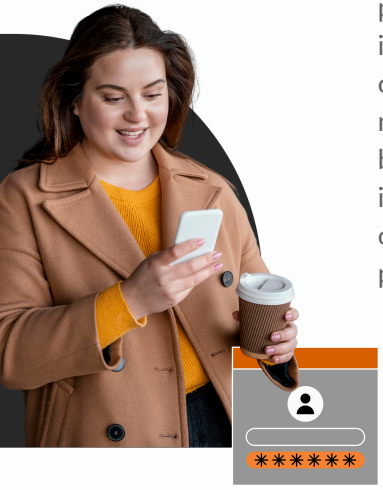
2. Invasão de conta

A invasão de conta, também conhecida como account takeover, ocorre quando alguém rouba a identidade de uma pessoa e realiza transações em suas contas bancárias.

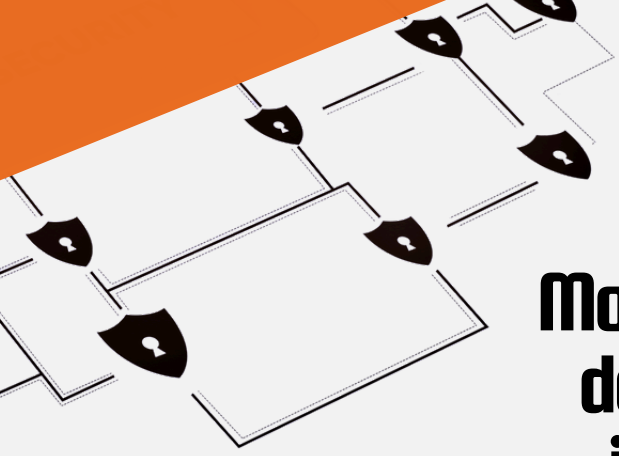
Na invasão de conta, um golpista utiliza bots de forma ilegal para obter acesso ao banco, ao site de comércio eletrônico ou a outros tipos de contas da vítima. Esse ataque resulta em transações fraudulentas e compras não autorizadas a partir da conta da vítima.

3. Roubo de identidade

O roubo de identidade envolve indivíduos que criam uma identidade falsa para enganar outras pessoas e obter benefícios financeiros.



O roubo de identidade ocorre quando alguém usa as informações de outra pessoa, como nome, número de identificação, número de cartão de crédito, número de seguridade social, número de carteira de motorista, conta bancária, PIN, assinaturas eletrônicas, impressões digitais, senhas ou qualquer outra informação que possa ser utilizada para acessar seus recursos financeiros.



Modalidades de roubo de identidade

Quando falamos sobre roubo de identidade, existem várias formas de operação. Entre as mais populares, encontramos:

- **Phishing:** é o roubo de dados por meio de e-mails. A técnica baseia-se no envio de links falsos para páginas da web que são similares aos sites que o usuário frequenta. Ou seja, cria-se uma réplica do site para que o usuário insira seus dados pessoais e, assim, obtê-los.

- **SMShing :** é o roubo de dados através de mensagens de texto ou SMS. Trata-se de uma fraude na qual são solicitados dados por meio de mensagens, ou é pedido que a pessoa ligue para um número específico ou acesse um site.

- **Vishing :** termo é uma combinação do inglês “voice” (voz) e phishing. É o roubo de dados através de chamadas telefônicas. Utiliza a linha telefônica convencional e técnicas de engenharia social para enganar pessoas e obter informações financeiras ou dados úteis para o roubo de identidade.

Essas modalidades visam pessoas vulneráveis, como idosos ou indivíduos de grupos sociais mais propensos a confiar nesse tipo de ação e acabar fornecendo dados importantes.

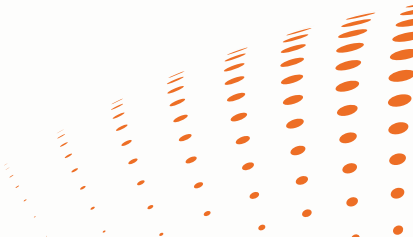
Mitigar esse tipo de ato é possível para os usuários se aplicarem medidas como:

- **Evitar** chamadas onde são solicitados dados.
- **Validar** a identidade de quem está entrando em contato em nome de entidades ou bancos.
- **Reportar** e-mails suspeitos como spam.
- **Não responder** mensagens ou e-mails suspeitos.
- **Não atender** e bloquear números desconhecidos.
- **Não fornecer** informações se não conhecer a origem de uma chamada ou e-mail e se estiverem solicitando dados sensíveis.

Malwares para obter informações

Os malwares são programas que se instalam no computador para roubar informações. Para evitá-los, os usuários devem:

- Comprar em sites com links seguros.
- Usar softwares de escaneamento e antivírus que garantam segurança durante a navegação.
- Manter sistemas operacionais atualizados.
- Ao pagar em uma loja física, não perder de vista o cartão.
- Ao comprar online, não salvar informações nas lojas.



Evitar ser vítima de fraudes depende dos nossos cuidados

Ao comprar pela internet, certifique-se de que o site é seguro e que utiliza uma plataforma de pagamento confiável e transparente.

Como evitar que seu negócio seja vítima de fraude

Ferramentas como o RiskCenter 360™ da Evertec são projetadas para controlar riscos e manter uma visibilidade completa sobre transações e pagamentos, identificando falhas para mitigá-las; além de se integrar ao protocolo 3DS para criar uma estratégia mista que combina técnicas de monitoramento e prevenção.

Esta ferramenta também permite analisar o comportamento dos clientes e suas transações, identificando anomalias e canais de uso. Isso é complementado com modelos de inteligência artificial e predição de dados.

Capacidades da plataforma

- Monitoramento e detecção de padrões suspeitos em diferentes meios de pagamento, incluindo transações com cartão presente e não presente.
- Análise em tempo real e quase em tempo real em diversos canais e dispositivos, como POS, caixas eletrônicos e comércio eletrônico.
- Envio de notificações aos titulares de cartões por múltiplos canais.
- Análise e documentação dos resultados de investigações de fraudes.
- Bloqueio preventivo ou permanente de cartões, contas, terminais e comércios, quando necessário.
- Auxilia instituições financeiras a atender requisitos regulatórios e normas da indústria, proporcionando uma visão completa e transparente do cliente e do processo de detecção de fraude.

Este sistema também facilita o monitoramento e análise de eventos não financeiros, como mudanças de endereço, atualização de dados e outros que podem ser negligenciados por outras ferramentas, pois não têm necessariamente um valor financeiro.

CONHEÇA NOSSAS
SOLUÇÕES

Soluções financeiras completas que elevam a **segurança** das suas transação financeira

evertec