Empresas & Negócios

Matéria de capa

Melpomenem_CANVA

CUIDADO COM A PROTEÇÃO

TENDÊNCIAS EM FRAUDES PARA 2025 E O FUTURO DOS GOLPES DIGITAIS

De acordo com um recente relatório da Kaspersky, o Brasil lidera a lista de países que mais sofrem ataques cibernéticos. Em 2025, espera-se que as empresas enfrentem um cenário no qual as ameaças cibernéticas se diversifiquem ainda mais, exigindo estratégias robustas e inovadoras para proteção de seus negócios e clientes.

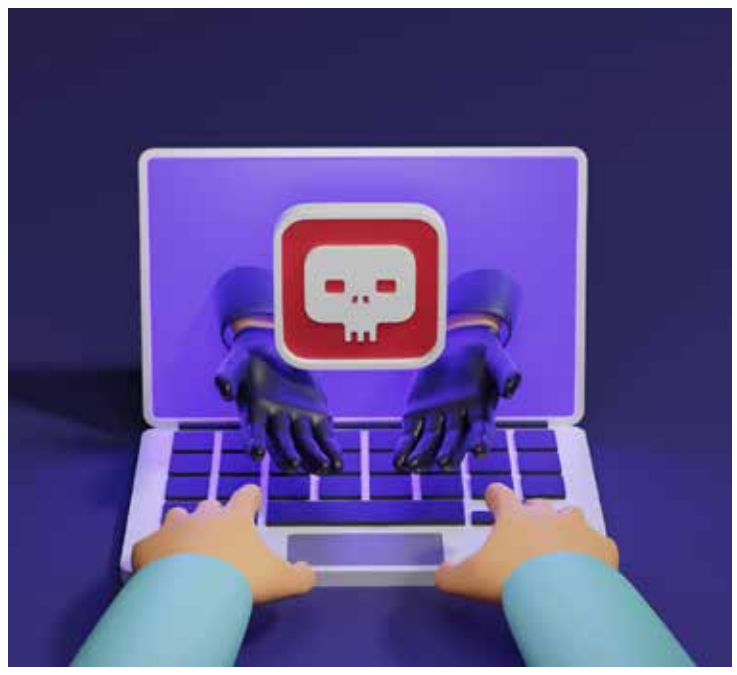
Thiago Bertacchini (*)

Segundo a Juniper Research, as perdas globais devido a fraudes online devem chegar perto dos $400 bilhões em 2025, impulsionadas por novos métodos de ataque e pela crescente digitalização de serviços. Esse cenário demanda uma postura mais proativa das empresas, que precisam investir em tecnologias avançadas de prevenção, bem como na conscientização de colaboradores e consumidores.

A abordagem reativa, focada apenas em responder a incidentes após sua ocorrência, já não é suficiente. A integração de ferramentas baseadas em inteligência artificial, aprendizado de máquina e sistemas de análise de comportamento em tempo real é fundamental para antecipar movimentos fraudulentos antes que eles causem prejuízos significativos.

A relação entre tecnologia e segurança – O avanço da tecnologia está no centro das tendências de fraude, mas também é a base das soluções para mitigá-las. Por exemplo, a implementação de IA generativa por criminosos está criando novos desafios: fraudes envolvendo deepfakes, como a manipulação de voz e vídeo para enganar sistemas de autenticação ou para aplicar golpes financeiros, são cada vez mais comuns.

Entretanto, essas mesmas tecnologias podem ser usadas para combater ataques. Modelos avançados de IA são capazes de detectar padrões irregulares em dados, como acessos suspeitos ou transações incompatíveis com o perfil do cliente, bloqueando ações fraudulentas em tempo real. Além disso, a segurança baseada em biometria comportamental, combinada com autenticação multifator (MFA), continuará sendo um pilar central da proteção digital.



Lerbank-bbk22_CANVA

Outro ponto crucial é a necessidade de equilibrar segurança com experiência do usuário. Estudos mostram que consumidores estão cada vez mais dispostos a adotar soluções de segurança robustas, desde que estas não prejudiquem a praticidade e a rapidez dos serviços digitais. Com base em relatórios de especialistas e tendências observadas, destacam-se os seguintes tipos de fraudes e ataques cibernéticos que devem ganhar relevância em 2025:

Fraudes baseadas em IA Generativa – O uso de ferramentas como ChatGPT - ou até o FraudGPT, para criminosos mais sofisticados - para criar comunicações fraudulentas altamente convincentes, além de deepfakes usados em fraudes financeiras e de identidade.

Ataques a carteiras digitais e sistemas de pagamento – Com o crescimento das carteiras digitais, estas se tornam alvos preferenciais. Técnicas como phishing e engenharia social sofisticada continuarão explorando falhas no comportamento humano para obtenção de credenciais de acesso e efetivação de golpes.

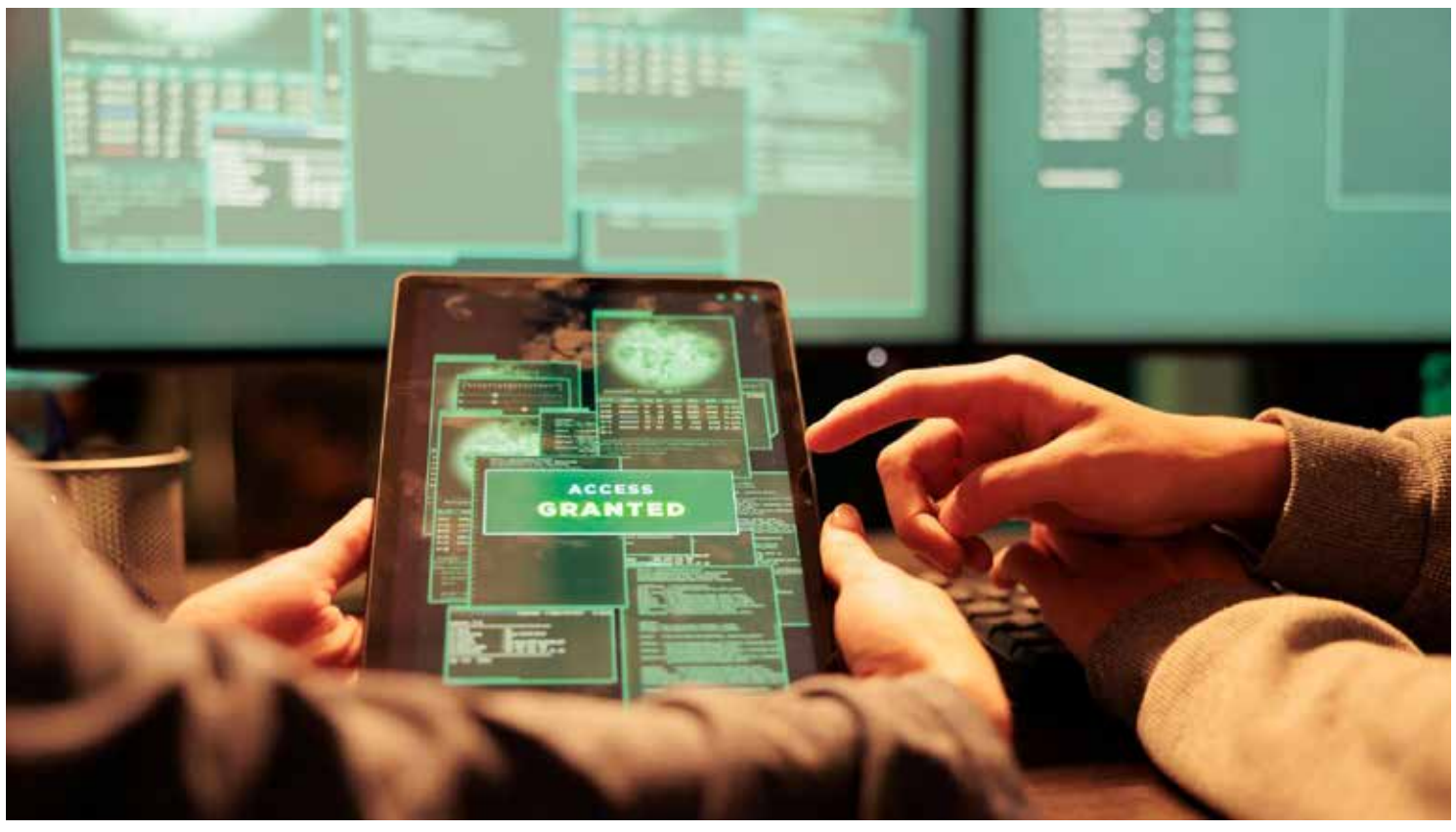
Ransomware mais avançado – Ataques com foco em extorsão, bloqueando sistemas e dados críticos das empresas, se tornarão mais direcionados e personalizados.

Golpes no comércio eletrônico e marketplaces – Fraudadores utilizarão técnicas como compras simuladas e manipulação de avaliações para enganar consumidores e empresas.

Exposição de APIs vulneráveis – Com a expansão do uso de APIs, os criminosos irão explorar brechas para obter acesso não autorizado a dados sensíveis.

Pagamentos Pix ou Conta a Conta – Com a popularidade do tipo de pagamento, os fraudadores continuam desenvolvendo malware (como o Pixpirate, por exemplo) e utilizam grandes campanhas de phishing e keylogging.

Para enfrentar essas ameaças, algumas estratégias tecnológicas são fundamentais: Implementação de modelos de IA preditiva, para antecipar padrões de comportamento anômalos; Tokenização e criptografia avançada, para proteger dados em trânsito e armazenados; Segurança centrada em APIs, garantindo o monitoramento e teste contínuo para evitar vulnerabilidades, e Zero Trust Architecture (ZTA), um modelo que assume a inexistência de confiança dentro e fora da rede, exigindo verificação rigorosa de cada solicitação de acesso.



Dragos_Condrea_CANVA

Atendendo à demanda do consumidor – Os consumidores exigem transações seguras, mas também fluidas. Uma pesquisa da Deloitte mostrou que 75% dos usuários abandonam plataformas que exigem processos de segurança excessivamente complicados. Assim, o futuro da prevenção à fraude deve garantir um equilíbrio entre eficiência operacional e experiência do cliente.

Empresas líderes estão investindo em soluções invisíveis para o consumidor, como monitoramento passivo e autenticação biométrica contínua, que elevam a segurança sem prejudicar a jornada do usuário. O cenário de fraudes para 2025 exige que empresas adotem uma mentalidade de segurança proativa, integrando tecnologia de ponta a processos e estratégias de proteção. A inovação tecnológica será tanto a origem dos novos desafios quanto a solução indispensável para superá-los.

Organizações que investirem em sistemas avançados de IA, automação e segurança, além de priorizarem a experiência do cliente, estarão mais preparadas para enfrentar os golpes digitais do futuro, protegendo não apenas seus negócios, mas também a confiança de seus clientes.

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