

OPINIÃO

Fraudes digitais expõem contradições da segurança bancária

Durante muito tempo, a segurança bancária foi apresentada como uma disputa tecnológica entre instituições financeiras e criminosos digitais, mas os golpes mais recentes começaram a expor uma contradição difícil de ignorar, o mesmo mecanismo que bloqueia um PIX de mil reais por considerar a movimentação fora do padrão muitas vezes libera empréstimos elevados, altera dispositivos de segurança e permite o esvaziamento completo da conta sem qualquer interrupção proporcional, ampliando a sensação de insegurança entre os clientes.

Nos últimos anos, o perfil das fraudes também mudou de maneira significativa, antes o criminoso tentava retirar a vítima do ambiente oficial do banco, conduzindo a pessoa para páginas falsas ou links suspeitos, agora a abordagem acontece dentro do próprio aplicativo legítimo da instituição, utilizando linguagem corporativa, validações reais e procedimentos comuns da rotina bancária, criando um grau de autenticidade extremamente difícil de distinguir da operação verdadeira e reduzindo a capacidade de reação diante da abordagem criminosas.

Relatos de vítimas passaram então a revelar um impacto que ultrapassa o prejuízo financeiro, casos como o da influenciadora e modelo Rarika Acler ajudam a mostrar como a fraude também afeta diretamente a confiança construída ao longo de anos de relacionamento com a instituição, após contatos de criminosos que se passaram pela área de segurança do banco, a influenciadora teve empréstimos e movimentações realizados em sequência dentro do próprio ambiente oficial da instituição, situação que levantou questionamentos sobre a capacidade de identificação de operações incompatíveis com o padrão histórico da conta.

A partir desse cenário, a discussão sobre golpes digitais começou a mudar de direção, a dúvida deixou de girar apenas em torno de como alguém caiu em uma fraude e passou a envolver outro ponto: o de porquê essas transações tão diferentes do comportamento habitual conseguem atravessar toda a estrutura de monitoramento sem uma checagem mais rigorosa, em

Olívia Flôres de Brás (*)

muitos casos uma simples transferência recebe travas automáticas, enquanto uma sequência envolvendo contratação de crédito, troca de senha, alteração de aparelho e retirada integral dos recursos acontece praticamente sem resistência operacional.

O debate ganha ainda mais peso na esfera jurídica, a Súmula 479 do Superior Tribunal de Justiça estabelece que bancos respondem por fraudes ligadas ao contexto operacional da atividade bancária, entendimento conhecido como fortuito interno, reconhecimento que parte do princípio de que determinados riscos fazem parte da própria atividade financeira e, justamente por isso, não podem ser transferidos integralmente para quem utiliza os serviços.

Na prática, porém, cresce a distância entre o discurso institucional e a experiência vivida no dia a dia. Os bancos investem bilhões em campanhas sobre segurança digital, enquanto milhares de pessoas seguem relatando abordagens semelhantes, contatos de falsos gerentes, supostas centrais de atendimento, alertas de bloqueio de conta, aplicações inexistentes, pedidos de resgate e até retirada de cartões por motoboys continuam aparecendo de maneira recorrente, mostrando que a atuação criminosa evolui em velocidade superior à sensação de proteção transmitida ao público.

Depois da fraude, o desconforto costuma aumentar ainda mais, muitas vítimas recebem respostas padronizadas afirmando que tudo aconteceu mediante uso de credenciais válidas, argumento que frequentemente desloca a discussão para a responsabilidade individual de quem sofreu o golpe, mesmo em situações nas quais a instituição permitiu contratação de crédito, alteração de segurança e movimentações atípicas logo após eventos considerados críticos.

Aos poucos, aumenta a percepção de que parte relevante do risco passou a ser transferida para o usuário final, bancos lucram com a digitalização, reduzem estruturas físicas, automatizam processos e diminuem o contato humano, mas quando a fraude acontece, a pessoa afetada frequentemente precisa provar sozinha que foi vítima dentro de um ambiente vendido como cada vez mais sofisticado e seguro, situação que amplia não apenas os prejuízos financeiros, mas também o desgaste contínuo da confiança nas instituições financeiras.

(*) CEO da Magno Investimentos.

Um novo símbolo de status: o notebook semiaberto

É cada vez mais comum ver pessoas circulando com seus notebooks semiabertos, em escritórios, aviões, restaurantes ou no Metro. O motivo? Não interromper o trabalho dos chamados “agentes de inteligência artificial”.

Vivaldo José Breternitz (*)

Um agente de inteligência artificial é um sistema autônomo capaz de executar tarefas de forma independente, utilizando modelos de inteligência artificial, softwares diversos e, evidentemente, dados.

A prática virou até motivo de ironia em um artigo do portal Business Insider e tem rendido memes, inclusive publicados pela OpenAI no TikTok.

No ambiente Windows, é possível configurar o notebook para funcionar mesmo com a tampa fechada. Já no ambiente Apple, isso é mais complicado e muitos preferem não arriscar. Resultado: mais pessoas circulando com seus notebooks semiabertos.

Essa prática, porém, traz riscos. O desgaste físico do equipamento é evidente: dobradiças sob pressão, quedas acidentais etc. Além disso, há problemas de segurança: notebooks são cobichados por ladrões, a privacidade é ameaçada e dados sensíveis podem ser vistos por terceiros. Em ambientes corporativos, isso pode abrir brechas para espionagem ou outras formas de cibercrime.

Os agentes de IA, por sua vez, avançam rapidamente. Hoje já geram conteúdo, classificam documentos, automatizam processos e até escrevem e corrigem softwares. Podem acessar a web, bancos de dados e aplicativos, operando de forma autônoma, o que nos permite acreditar que cada vez mais gente vai circular com seus notebooks semiabertos, ainda mais porque muitos acreditam ser isso um sinal de status...

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.



Copilot

Brasileiros ampliam presença em mercado de criptomoedas, mas medo ainda limita investimentos

O número de brasileiros que investem ou já investiram em criptomoedas cresce de forma consistente. Estimativas apontam que cerca de 59 milhões de pessoas no país já tiveram contato com esses ativos, o equivalente a aproximadamente 37% da população adulta. Entre os investidores, 42% afirmam já ter comprado criptomoedas ao menos uma vez, segundo levantamentos do setor.



Divulgação

O volume financeiro também confirma a expansão do mercado. Entre julho de 2024 e junho de 2025, o Brasil movimentou cerca de US\$ 318,8 bilhões (aproximadamente R\$ 1,7 trilhões) em criptomoedas, um crescimento de 109,9% em relação ao período anterior. Com esse desempenho, o país se consolidou como líder do mercado cripto na América Latina e ocupa atualmente a quinta posição no ranking global de adoção desses ativos, considerando volume de transações, número de usuários e uso em pagamentos e investimentos.

Dados recentes mostram um avanço no perfil do investidor e na regionalização do mercado de ativos digitais no Brasil. Segundo o relatório “Raio-X do Investidor de Ativos Digitais 2025”, o setor cresceu 43% em 2025, enquanto o investimento médio por usuário ultrapassou R\$ 5,7 mil. O estudo também aponta que cerca de 18% dos investidores já

diversificam aplicações em mais de um ativo digital. A região Sudeste concentra a maior parte das negociações, com destaque para São Paulo e Rio de Janeiro. Jovens de até 24 anos lideraram a expansão do mercado, com crescimento de 56% na participação, enquanto Bitcoin, Tether, Ethereum e Solana figuraram entre os ativos mais negociados no país.

Apesar da adesão crescente, o medo ainda é um fator importante para muitos brasileiros. A principal barreira está na falta de conhecimento sobre como funcionam os criptoativos e as tecnologias associadas, como blockchain e carteiras digitais. “Grande parte das pessoas ainda vê a criptomoeda como algo complexo

ou pouco transparente. Quando o investidor não entende exatamente como funciona, a tendência natural é evitar esse tipo de investimento”, afirma Cleverson Pereira, head de educação da OniIX.

Outro fator que reforça a desconfiança é o histórico de fraudes e esquemas associados ao setor, além da alta volatilidade do mercado. Variações bruscas de preço podem gerar a percepção de risco elevado e dificultar a compreensão do valor real dos ativos. Para Pereira, o avanço da regulamentação e da educação financeira tende a reduzir essas barreiras. “O Brasil tem potencial para se tornar um dos maiores mercados cripto do mundo. Mas a confiança do investidor virá menos da tecnologia em si e mais de educação financeira, informação qualificada e segurança institucional”, conclui.

Educação contínua e expansão
Com uma operação intuitiva e flexível, semelhante às plataformas de streaming, a AVO Educacional oferece videoaulas de curta duração, entre 8 e 15 minutos, garantindo foco e retenção de conteúdo. “Mais do que conversar com nossos clientes e assessores, buscamos oferecer uma linguagem única e democrática para todos que queiram aprender sobre esses temas”, diz Pereira.



News@TI

theGarage projeta R\$3,2 milhões com novo ecossistema de IA

@O theGarage, criado pela empresa de soluções em tecnologia Nexnux, estruturou uma nova frente de negócios voltada à aplicação prática de inteligência artificial nas empresas e projeta alcançar cerca de R\$3,2 milhões em contratos recorrentes até 2027. A iniciativa, chamada theGarage IA, funciona como um ecossistema integrado que combina diagnóstico, capacitação e desenvolvimento de soluções sob medida, com foco em tornar o uso da IA mais estruturado, seguro e sustentável dentro das organizações. O movimento marca uma evolução no posicionamento da companhia, que ao longo dos últimos anos transitou entre projetos sob demanda, desenvolvimento de produtos e criação de startups. A nova frente é organizada em três pilares principais: Hub de IA & Negócios, IA

Lab e Studio IA, que atuam de forma complementar ao longo da jornada das empresas.

Z.ro anuncia aquisição da fintech Paag

@O Z.ro Global Payments, que até abril operava como Z.ro Bank, anuncia a aquisição e incorporação da vertical de pagamentos da Paag, em um movimento estratégico voltado à consolidação de mercado e ao ganho de participação no setor de pagamentos digitais. A integração será realizada por meio de um plano estruturado de migração, desenhado para assegurar continuidade operacional, com estabilidade e segurança para todos os clientes ao longo do processo. “A criação dessa frente específica reflete a relevância do segmento e da necessidade de criar soluções cada vez mais customizadas para este mercado. Nossos dois novos sócios trazem um know-how essencial para liderar esta frente”, afirma o CEO da Z.ro Global Payments.