

Itaú Unibanco alerta para golpes com deepfakes e reforça orientações de segurança digital

Com o avanço do uso de Inteligência Artificial em tentativas de fraude, banco destaca medidas de proteção e reforça cuidados para clientes evitarem golpes

São Paulo, junho de 2026 – O avanço da Inteligência Artificial tem ampliado a sofisticação das tentativas de fraude digital no Brasil e no mundo. Entre os golpes que vêm ganhando relevância estão aqueles que utilizam deepfakes, clonagem de voz e outras formas de manipulação de imagem, vídeo e áudio para simular situações reais e induzir vítimas a realizar transferências ou compartilhar dados pessoais.

Atento a esse cenário, o Itaú Unibanco reforça sua atuação em prevenção a golpes e fraudes, combinando tecnologia, análise de comportamento, governança de dados e ações permanentes de conscientização para apoiar clientes e a sociedade no enfrentamento a esse tipo de ameaça.

De acordo com o relatório global FBI IC3 Crime Report, as perdas associadas a crimes digitais chegaram a US\$ 20,8 bilhões em 2025, o equivalente a cerca de R\$ 115 bilhões. Desse total, 85% estiveram relacionados a fraudes digitais, e quase US\$ 893 milhões, aproximadamente R\$ 4,9 bilhões, tiveram algum tipo de uso de Inteligência Artificial como parte da abordagem criminosa.

“As ferramentas de Inteligência Artificial tornaram os golpes mais sofisticados, especialmente quando combinadas com técnicas de engenharia social. Muitas vezes, o objetivo do criminoso não é criar uma fraude tecnicamente perfeita, mas gerar urgência, confiança ou medo para levar a vítima a tomar uma decisão precipitada. Por isso, atuamos de forma preventiva, com camadas de segurança que analisam contexto, comportamento e sinais de risco antes e durante a jornada do cliente”, afirma **Felipe Tambelini, diretor de Prevenção a Fraudes do Itaú Unibanco**.

No Brasil, ataques envolvendo deepfakes cresceram 126% em 2025, enquanto os golpes de personificação, quando o criminoso se passa por outra pessoa, registraram alta de 140%, segundo dados divulgados pela Biocatch. O tema também preocupa os consumidores: 89% dos brasileiros afirmam temer ter sua voz clonada por ferramentas de Inteligência Artificial.

“Investimos continuamente em tecnologia e inteligência aplicada à prevenção a golpes e fraudes, sempre considerando a realidade dos nossos clientes e os principais tipos de

golpes observados no mercado brasileiro. Além das soluções de segurança, também temos o compromisso de orientar a população, já que informação é uma das principais formas de proteção”, completa Tambelini.

Como os golpes com IA funcionam

Criminosos têm utilizado ferramentas de Inteligência Artificial para criar áudios, vídeos, imagens ou mensagens falsas que simulam situações legítimas. Essas abordagens costumam explorar sentimentos como urgência, medo ou confiança na mensagem para convencer a vítima a realizar transferências, informar senhas, compartilhar códigos de segurança ou liberar acessos.

Entre as principais modalidades associadas ao uso de IA, destacam-se:

Golpe da falsa central: o fraudador se passa por funcionário do banco ou por uma central de atendimento falsa. Com apoio de recursos de clonagem de voz ou roteiros personalizados, tenta convencer o cliente de que há uma suposta movimentação suspeita na conta e solicita transferências, senhas, códigos de segurança, dados do cartão ou instalação de aplicativos.

Golpe do falso advogado ou falso parente: criminosos usam informações disponíveis publicamente, inclusive amostras de voz em redes sociais, para simular a voz de familiares, conhecidos ou profissionais contratados. Em geral, alegam situações de emergência, processos judiciais ou pagamentos urgentes para induzir a vítima a realizar transferências.

Como o Itaú atua para proteger os clientes

Para apoiar os clientes na prevenção a golpes, o Itaú disponibiliza no Superapp a Área de Segurança, que reúne funcionalidades voltadas à proteção da conta e do cartão, e à gestão autônoma de recursos de segurança.

Entre as soluções disponíveis está o Modo Protegido, que permite ao cliente definir limites para transações realizadas fora de locais seguros. Outra funcionalidade é o Alerta Pix, que utiliza inteligência em tempo real para identificar transferências atípicas e alertar o cliente antes da conclusão da operação

Além das camadas tecnológicas de proteção, o Itaú reforça orientações importantes de segurança: o banco nunca solicita que clientes façam transferências, estornos ou pagamentos para resolver supostos problemas na conta. O Itaú também não pede senhas, códigos de segurança, iToken, dados do cartão ou instalação de aplicativos por telefone, mensagem ou e-mail.

Em caso de ligação ou mensagem suspeita, especialmente quando houver pedido de dinheiro urgente, transferência, atualização cadastral ou compartilhamento de dados, a recomendação é interromper o contato imediatamente e procurar os canais oficiais do banco.

Sobre o Itaú Unibanco

O Itaú Unibanco é o maior banco privado da América Latina em volume de receita e carteira de crédito, com presença em 18 países e mais de 70 milhões de clientes. Como banco universal, atua de forma integrada em Varejo, Atacado e Investimentos, oferecendo soluções financeiras para pessoas, empreendedores e empresas de diferentes portes. O banco possui posição de liderança em segmentos como alta renda e agronegócio e investe continuamente em tecnologia e inovação – com uso intensivo de dados e Inteligência Artificial – para aprimorar a experiência dos clientes e ampliar sua atuação consultiva. Seu propósito é promover o bem-estar financeiro e contribuir para a prosperidade do país, apoiando clientes com soluções e assessoria em suas jornadas de crescimento, inclusão social e transição para uma economia de baixo carbono.

Itaú Unibanco – Comunicação Corporativa imprensa@itau-unibanco.com.br