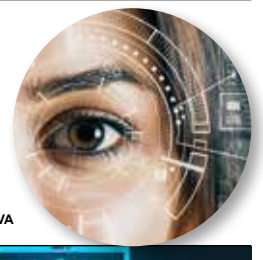
Empresas & Negócios

Matéria de capa



Blue_Planet_Studio_CANVA

BIOMETRIA NÃO É SUFICIENTE

COMO FRAUDES AVANÇADAS ESTÃO DESAFIANDO OS BANCOS

A adoção de biometria explodiu no Brasil nos últimos anos – 82% dos brasileiros já utilizam alguma tecnologia biométrica para autenticação, impulsionada pela conveniência e pela busca por mais segurança nos serviços digitais. Seja no acesso a bancos via reconhecimento facial ou no uso de impressão digital para autorizar pagamentos, a biometria virou o "novo CPF" em termos de identificação pessoal, tornando processos mais rápidos e intuitivos.

Sylvio Sobreira Vieira (*)

Porém, uma onda crescente de fraudes tem exposto os limites dessa solução: somente em janeiro de 2025, foram registradas 1,24 milhão de tentativas de fraude no Brasil, um aumento de 41,6% em relação ao ano anterior – o equivalente a uma tentativa de golpe a cada 2,2 segundos. Grande parte desses ataques mira justamente os sistemas de autenticação digital. Dados da Serasa Experian mostram que em 2024 as tentativas de fraude contra bancos e cartões cresceram 10,4% em relação a 2023, representando 53,4% de todas as fraudes registradas no ano.

Se não tivessem sido evitadas, essas fraudes poderiam ter causado um prejuízo estimado em R$ 51,6 bilhões. Esse aumento reflete uma mudança de cenário: os golpistas estão evoluindo suas táticas mais rápido do que nunca. Segundo uma pesquisa da Serasa, metade dos brasileiros (50,7%) foi vítima de fraudes digitais em 2024, um salto de 9 pontos percentuais em relação ao ano anterior, e 54,2% dessas vítimas sofreram prejuízo financeiro direto.

Outra análise aponta um aumento de 45% nos crimes digitais em 2024 no país, com metade das vítimas sendo efetivamente ludibriadas pelos golpes. Diante desses números, a comunidade de segurança questiona: se a biometria prometia proteger usuários e instituições, por que os fraudadores parecem estar sempre um passo à frente?

Golpes driblam reconhecimento facial e digital

Parte da resposta está na criatividade com que as quadrilhas digitais contornam os mecanismos biométricos. Nos últimos meses, surgiram casos emblemáticos. Em Santa Catarina, um grupo fraudulento lesou pelo menos 50 pessoas obtendo clandestinamente dados de biometria facial de clientes – um funcionário de telecomunicações simulou vendas de linhas telefônicas para capturar selfies e documentos dos clientes, usando esses dados depois para abrir contas bancárias e contrair empréstimos em nome das vítimas.

Em Minas Gerais, criminosos foram além: fingiram ser entregadores dos Correios para coletar impressões digitais e fotos de moradores, com o objetivo expresso de burlar a segurança de bancos. Ou seja, os golpistas não só atacam a tecnologia em si, mas também exploram a engenharia social – induzindo pessoas a entregarem seus próprios dados biométricos sem perceber. Especialistas alertam que mesmo sistemas considerados robustos podem ser enganados.

O problema é que a popularização da biometria criou uma falsa sensação de segurança: os usuários presumem que, por ser biométrica, a autenticação é infalível.

Em instituições com barreiras menos rigorosas, golpistas conseguem êxito usando meios relativamente simples, como fotos ou moldes para imitar características físicas. O chamado "golpe do dedo de silicone", por exemplo, tornou-se conhecido: criminosos colam películas transparentes

Divulgação

Sylvio Sobreira Vieira

em leitores de digitais de caixas eletrônicos para roubar a impressão do cliente e depois criam um dedo falso de silicone com aquela digital, realizando saques e transferências indevidas. Bancos afirmam já empregar contramedidas – sensores capazes de detectar calor, pulsação e outras características de um dedo vivo, inutilizando moldes artificiais.

Ainda assim, casos isolados desse golpe evidenciam que nenhuma barreira biométrica está totalmente a salvo de tentativa de burlar. Outro vetor preocupante é o uso de ardis de engenharia social para obter selfies ou exames faciais dos próprios clientes. A Federação Brasileira de Bancos (Febraban) soou o alarme para um novo tipo de fraude em que golpistas solicitam "selfies de confirmação" às vítimas sob falsos pretextos. Por exemplo, fingindo serem funcionários de banco ou do INSS, eles pedem uma foto do rosto "para atualizar cadastro" ou liberar um benefício inexistente – na verdade, usam essa selfie para se passar pelo cliente em sistemas de verificação facial.

Um simples descuido – como tirar uma foto atendendo ao pedido de um suposto entregador ou agente de saúde – pode fornecer aos criminosos a "chave" biométrica para acessar contas alheias.

Deepfakes e IA: a nova fronteira dos golpes

Se enganar pessoas já é uma estratégia muito utilizada, os criminosos mais avançados estão também enganando as máquinas. Aqui entram as ameaças de deepfake – manipulação avançada de voz e imagem por inteligência artificial – e outras técnicas de falsificação digital que tiveram um salto de sofisticação de 2023 para 2025.

Em maio passado, por exemplo, a Polícia Federal deflagrou a operação "Face Off" após identificar um esquema que fraudou cerca de 3 mil contas do portal Gov.br usando biometria facial falsa. O grupo criminoso aplicava técnicas altamente sofisticadas para se passar por usuários legítimos na plataforma gov.br, que concentra o acesso a milhares de serviços públicos digitais.

Investigadores revelaram que os golpistas usavam uma combinação de vídeos manipulados, imagens alteradas por IA e até máscaras 3D hiper-realistas para enganar o mecanismo de reconhecimento facial. Em outras palavras, simulavam os traços faciais de terceiros – inclusive pessoas já falecidas – para assumirem identidades e acessar benefícios financeiros vinculados àquelas contas. Com movimentos artificiais de piscar olhos, sorrir ou virar a cabeça sincronizados perfeitamente, conseguiam até driblar a funcionalidade de liveness detection, que foi desenvolvida exatamente para detectar se há uma pessoa real diante da câmera.

O resultado foi o acesso indevido a valores que deveriam ser resgatados apenas pelos verdadeiros beneficiários, além da aprovação ilícita de empréstimos consignados no app Meu INSS usando essas identidades falsas. Esse caso expôs de forma contundente que sim, é possível burlar a biometria facial – mesmo em sistemas grandes e teoricamente seguros – quando se dispõe das ferramentas certas.

No setor privado, a situação não é diferente. Em outubro de 2024, a Polícia Civil do Distrito Federal conduziu a operação "DeGenerative AI", desarticulando uma quadrilha especializada em invadir contas de bancos digitais por meio de apps de inteligência artificial. Os criminosos realizaram mais de 550 tentativas de invasão de contas bancárias de clientes, usando dados pessoais vazados e técnicas de deepfake para reproduzir a imagem dos correntistas e assim validar procedimentos de abertura de novas contas em nome das vítimas e habilitar dispositivos móveis como se fossem delas.

Estima-se que o grupo tenha conseguido movimentar cerca de R$ 110 milhões em contas de pessoas físicas e jurídicas, lavando dinheiro de diversas origens, antes que a maioria das fraudes fosse barrada pelas auditorias internas dos bancos.

Para além da biometria

Para o setor bancário brasileiro, a escalada desses golpes de alta tecnologia acende um sinal de alerta. Os bancos investiram pesado na última década para migrar clientes para canais digitais seguros, adotando biometria facial e digital como barreiras contra fraude.

Entretanto, a recente onda de golpes sugere que depender exclusivamente da biometria pode não ser suficiente. Golpistas exploram falhas humanas e brechas tecnológicas para se passar pelos consumidores, e isso demanda com que a segurança seja pensada em múltiplos níveis e fatores de autenticação, não mais um único fator "mágico".

Diante desse cenário complexo, especialistas convergem em uma recomendação: adotar autenticação multifator e abordagens multicamadas de segurança. Isso significa combinar diferentes tecnologias e métodos de verificação, de forma que, se um fator falhar ou for comprometido, outros impeçam a fraude. A própria biometria continua sendo peça importante – afinal, quando bem implementada com verificação de vida (liveness) e criptografia, dificulta bastante ataques oportunistas.

Porém, deve atuar junto com outros controles: senhas ou PINs de uso único enviados ao celular, análise de comportamento do usuário – a chamada biometria comportamental, que identifica padrões de digitação, uso do aparelho e pode soar o alarme ao notar um cliente "agindo diferente do normal" –, e monitoramento inteligente de transações.

Ferramentas de IA também estão sendo usadas a favor dos bancos, identificando sinais sutis de deepfake em vídeos ou vozes – por exemplo, analisando frequências de áudio para detectar vozes sintéticas ou procurando distorções visuais em selfies.

No fim das contas, a mensagem que fica para os gestores bancários e profissionais de segurança da informação é clara: não existe bala de prata. A biometria trouxe um patamar superior de segurança em comparação com senhas tradicionais – tanto que os golpes migraram em boa parte para enganar as pessoas, não mais quebrar algoritmos.

Contudo, os fraudadores estão explorando cada brecha, seja humana ou tecnológica, para frustrar os sistemas biométricos. A resposta adequada envolve tecnologia de ponta em constante atualização e monitoramento proativo. Só quem conseguir evoluir suas defesas na mesma velocidade em que surgem novos golpes estará apto a proteger plenamente seus clientes na era da inteligência artificial maliciosa.

Melpomenem_CANVA

(*) CEO & Head Consulting da SVX Consultoria.