

Itaú Unibanco alerta para golpe da coleta indevida de dados biométricos

Criminosos utilizam táticas de engenharia social para induzir vítimas a compartilharem dados biométricos; banco mostra como identificar e evitar esse tipo de golpe

Setembro de 2025 – O Itaú Unibanco chama a atenção para um golpe sofisticado envolvendo a coleta indevida de dados biométricos, utilizados por criminosos para fraudes financeiras. Esse tipo de abordagem inclui argumentos enganosos – como promessas de brindes promocionais e alegações de fraudes inexistentes – para capturar a confiança das vítimas e justificar a solicitação de dados sensíveis, como reconhecimento facial e impressão digital. A maior incidência de ocorrência desse tipo está nos estados de São Paulo e Rio de Janeiro, mas o alerta se estende a todo o país.

Victor Thomazetti, superintendente de Prevenção a Fraudes do Itaú Unibanco, explica que os golpistas utilizam métodos cada vez mais sofisticados para manipular as vítimas. “A engenharia social está mais avançada devido às tecnologias emergentes e à vasta disponibilidade de dados disponíveis na internet. Os criminosos utilizam narrativas muito convincentes, que exploram gatilhos emocionais, como urgência e medo, para fazer com que as pessoas acreditem na legitimidade das solicitações. No caso da biometria, os golpistas estruturam um discurso que faz a vítima acreditar que fornecer esses dados é indispensável. O que recomendamos é: pare, pense e questione. Essa pausa crítica pode evitar o golpe”, afirma.

O executivo também esclarece os mitos sobre a biometria e destaca os esforços do banco para proteger seus clientes. “A biometria, além de ser uma tecnologia extremamente segura, oferece uma experiência simplificada baseada em inteligência artificial avançada. No entanto, justamente por sua confiabilidade, se torna alvo de criminosos que buscam enganar as pessoas para obter acesso indevido. A conscientização é um pilar essencial da nossa estratégia, e acreditamos que experiência e segurança devem caminhar juntas”, conclui Thomazetti.

Diante desse cenário, é essencial que os consumidores adotem práticas preventivas e fiquem atentos às abordagens suspeitas.

- 1. Forneça dados biométricos apenas em canais oficiais**
Nunca compartilhe dados sensíveis, como sua biometria ou informações bancárias, fora de ambientes digitais ou físicos controlados e confiáveis.
- 2. Desconfie de abordagens que oferecem brindes em troca de dados pessoais**
Promoções legítimas não exigem o compartilhamento de dados sensíveis para o recebimento de brindes ou prêmios.
- 3. Confirme diretamente com a instituição**

Caso suspeite de fraude, entre em contato imediatamente com o serviço oficial da instituição financeira para verificar a situação.

4. E, caso tenha sido vítima de golpe ou fraude...

Além do contato com a instituição financeira para tomar as providências cabíveis, faça um boletim de ocorrência na delegacia de polícia mais próxima.

Para orientar a população sobre boas práticas de segurança, o Itaú desenvolve materiais de conscientização e disponibiliza um canal com informações sobre prevenção que pode ser acessado pelo [site](#) oficial.

Amigos e familiares podem ajudar no bloqueio de contas e cartões pós roubo ou furto

Você sabia que qualquer pessoa pode solicitar o bloqueio da conta ou cartões de um amigo ou parente que passou por uma situação de roubo ou furto? Basta ligar para a Central de Atendimento do Itaú Unibanco com o CPF da vítima em mãos e seguir o passo a passo. O processo é simples e rápido e você contribui com a prevenção contra golpes e fraudes.

Central de Atendimento Itaú Unibanco

4004-4828 – capitais e regiões metropolitanas

0800-970-4828 – demais localidades

Além disso, o banco oferece uma página dedicada ao tema, onde você pode conhecer mais sobre o assunto e compartilhar com amigos e familiares. Acesse itau.com.br/seguranca e confira!

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