Golpe da falsa central avança com estratégias mais sofisticadas para abordar clientes, reforça Itaú Unibanco

Banco orienta clientes a desconfiar de contatos que solicitem senhas, códigos de segurança, instalação de aplicativos ou transferências para suposta proteção da conta

São Paulo, agosto de 2026 – Com abordagens cada vez mais sofisticadas, o golpe da falsa central segue entre as principais modalidades de engenharia social usadas contra clientes do sistema financeiro. O golpe costuma começar com um contato, por telefone ou mensagem, sobre uma situação que gera preocupação, como uma suposta compra suspeita, tentativa de invasão da conta ou movimentação fora do padrão. Em seguida, o falso funcionário do banco pede senhas, código iToken, instalação de aplicativos ou transferência de valores para uma "conta segura".

O alerta ocorre em um cenário de alta dos crimes de estelionato no País. Segundo o Anuário Brasileiro de Segurança Pública, divulgado pelo Fórum Brasileiro de Segurança Pública, o Brasil registrou 2,2 milhões de casos em 2025, média de quatro golpes por minuto. Entretanto, como 15% da população adulta brasileira declarou ter sido vítima de golpe, há um risco de subnotificação e esse número pode chegar a até 20 milhões de ações criminosas. Já as fraudes digitais ultrapassaram 346 mil ocorrências, avanço de 20,6% na comparação anual.

"O golpe da falsa central é construído para parecer um contato legítimo. As pessoas criminosas podem citar informações parciais sobre o cliente para ganhar credibilidade. Nas ligações, simulam transferências entre departamentos, usam músicas de espera e podem mascarar o número de origem da chamada com a técnica de "call spoofing,", que permite mostrar um número falso na tela do dispositivo da vítima. Por isso, o principal sinal de alerta está no pedido feito ao cliente. Bancos não solicitam senha, iToken, dados do cartão ou transferência de valores para proteger a conta do cliente", afirma Ana Leda Guedes Tavares, superintendente de Prevenção a Fraudes do Itaú Unibanco.

Esse tipo de abordagem combina a autoridade percebida da instituição financeira e a sensação de urgência criada durante o contato. Ao acreditar que está recebendo uma orientação oficial, a vítima pode acabar compartilhando dados sensíveis ou realizando ações que normalmente não faria. Ao mesmo tempo, as pessoas criminosas pressionam por decisões rápidas, o que reduz o tempo disponível para reflexão e aumenta as chances de sucesso do golpe.

O que deve acender o alerta durante o contato

Embora as narrativas variem, a orientação é interromper o contato e buscar os canais oficiais sempre que houver pedidos como:

- **Solicitação de dados sensíveis:** pedidos de senhas, código iToken, dados do cartão, QR Code ou fotos e selfies de validação biométrica.

- **Transferências financeiras:** orientação para realizar Pix, depósitos, estornos ou movimentar valores para uma suposta "conta segura".
- **Instalação de programas:** pedidos para baixar aplicativos de acesso remoto, softwares ou clicar em links enviados por mensagem durante a chamada.
- **Pressão por sigilo ou continuidade:** pedidos para não encerrar a chamada, não procurar a agência física ou não conferir as informações pelo aplicativo do banco.

O Itaú Unibanco reforça que esses pedidos não fazem parte dos procedimentos de atendimento dos bancos.

Como agir em caso de suspeita ou fraude

Em caso de contato suspeito ou golpe, a recomendação é agir rapidamente:

1. **Interrompa a chamada imediatamente:** não há necessidade de prosseguir no telefone para "confirmar" o problema. Desligue e acione o banco por meio de canais oficiais.
2. **Confirme pelos canais oficiais:** entre em contato pelo chat do aplicativo ou pelos telefones disponíveis no site oficial (itau.com.br/seguranca) e desconsidere números informados durante a abordagem suspeita.
3. **Comunique o banco e preserve evidências:** caso tenha compartilhado dados ou realizado transações, avise a instituição financeira e guarde comprovantes, números chamadores e capturas de tela.
4. **Registre o Boletim de Ocorrência:** a formalização na Polícia Civil ajuda na investigação de redes criminosas e no combate contínuo a golpes no País.

Tecnologia aliada à conscientização: Alerta Pix

Para prevenir golpes, o Superapp do Itaú conta com o **Alerta Pix**, funcionalidade que usa inteligência de dados em tempo real para identificar transações suspeitas. Quando detecta uma operação com características de risco, o app exibe um aviso antes da conclusão da transferência.

A iniciativa busca criar uma pausa no momento da transação, dando mais contexto e tempo para que o cliente avalie a operação. O Alerta Pix se soma às demais ferramentas de proteção do banco, fortalecendo as ações de conscientização realizadas pelo Itaú para uma tomada de decisão mais segura.

Central de Atendimento Itaú Unibanco

4004-4828 – capitais e regiões metropolitanas

0800-970-4828 – demais localidades

Página oficial de segurança: itau.com.br/seguranca

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