

Golpes por site falso, WhatsApp e redes sociais lideram contestações



Levantamento do banco sobre o primeiro semestre de 2026 aponta os principais tipos de fraude relatados por clientes e reforça orientações para evitar prejuízos.

Os golpes de engenharia social estão cada vez mais sofisticados e personalizados. No primeiro semestre de 2026, os golpes envolvendo sites falsos, WhatsApp e redes sociais apareceram entre os tipos de fraude mais comunicados por clientes do Santander.

Segundo o levantamento da instituição, criminosos têm utilizado diferentes canais para se passar por empresas, familiares e até funcionários de bancos. As abordagens buscam obter dados pessoais e bancários ou induzir as vítimas a realizar transferências e pagamentos.

De acordo com Leandro Granja, CISO do Santander, um dos principais desafios está em proteger o cliente justamente no momento em que ele é pressionado a tomar uma decisão. Por isso, o banco afirma ter ampliado o uso de alertas preventivos e mecanismos adicionais de confirmação durante transações consideradas sensíveis.

Falsa central ganha novas abordagens

Outro golpe que aparece no levantamento é o da falsa central de atendimento. Segundo o Santander, os criminosos passaram a utilizar novas estratégias, incluindo mensagens pelo WhatsApp que simulam procedimentos como “prova de vida”, bloqueio do ID Santander e supostas validações de segurança.

A estratégia combina técnicas de persuasão com informações sobre as vítimas e simulação de atendimentos legítimos para aumentar a credibilidade da abordagem.

O banco afirma que mantém investimentos contínuos em tecnologia, monitoramento e prevenção. A instituição utiliza recursos como machine learning, biometria comportamental, análise de transações em tempo real, identificação de sinais do dispositivo e monitoramento 24 horas por dia.

Entre as ferramentas citadas estão a biometria facial com inteligência artificial, mecanismos de autenticação, alertas de segurança nos aplicativos Santander e Santander Empresas e confirmações de compras suspeitas por WhatsApp, notificações push ou SMS.

Confira os cinco golpes mais contestados

Segundo o levantamento do Santander referente ao primeiro semestre de 2026:

Site falso

WhatsApp

Redes sociais

Falso investimento

Falsa central

Como evitar cair nos principais golpes

Site falso

Criminosos criam páginas que imitam lojas, bancos e outros serviços conhecidos para induzir o usuário a fornecer informações ou realizar pagamentos.

Como se proteger:

Desconfie de promoções muito vantajosas e confirme a oferta no site ou aplicativo oficial.

Evite clicar em links e anexos enviados por contatos desconhecidos ou suspeitos.

Confira cuidadosamente o endereço do site antes de inserir qualquer informação.

Golpe do WhatsApp

Nesse tipo de fraude, criminosos utilizam fotos de familiares ou conhecidos e afirmam ter trocado de número. Em seguida, pedem transferências via Pix alegando situações urgentes.

Como se proteger:

Confirme por ligação se a pessoa realmente mudou de número.

Ative a confirmação em duas etapas no WhatsApp.

Desconfie de pedidos acompanhados de pressão ou urgência.

Golpes nas redes sociais

Perfis podem ser invadidos ou utilizados para divulgar ofertas falsas, produtos com preços muito abaixo do mercado e oportunidades de ganhos rápidos.

Como se proteger:

Desconfie de promessas de dinheiro fácil ou ofertas muito abaixo do preço habitual.

Confira promoções diretamente no site oficial da empresa.

Ative a autenticação em duas etapas nas redes sociais.

Falso investimento

Golpistas oferecem supostos investimentos com alta rentabilidade e podem se passar por funcionários de bancos ou corretoras. Para tornar a fraude mais convincente, utilizam informações pessoais, relatórios falsos e contatos por diferentes canais.

Como se proteger:

Desconfie de promessas de dinheiro rápido e fácil.

Não tome decisões financeiras sob pressão.

Verifique a instituição e a legitimidade da oferta antes de investir, utilizando fontes oficiais, como a Comissão de Valores Mobiliários (CVM).

Falsa central

Criminosos se apresentam como funcionários de instituições financeiras e alegam identificar movimentações suspeitas na conta. Durante o contato, podem solicitar senhas, códigos, dados pessoais ou até orientar a vítima a realizar uma transação para supostamente cancelar uma operação.

Como se proteger:

O Santander orienta que não solicita transações para cancelar compras suspeitas ou Pix indevidos.

Não forneça senhas, códigos de segurança, dados bancários ou informações pessoais por telefone.

Não siga instruções para realizar procedimentos em caixas eletrônicos com o objetivo de “cancelar” operações.

Desconfie de solicitações para instalar programas, compartilhar códigos ou fotografar QR Codes.

Informação e atenção são importantes

Com o avanço das técnicas utilizadas pelos criminosos, a recomendação é interromper o contato diante de qualquer abordagem suspeita e buscar os canais oficiais da instituição ou empresa envolvida.

Na dúvida, pare, confira a informação e não realize nenhuma transferência ou pagamento antes de confirmar a solicitação.

Foto: Divulgação

<https://jornalpanfletus.com.br/cp3.masterix.inf.br/noticia/8851/golpes-por-site-falso-whatsapp-e-redes-sociais-lideram-contestacoes> em 22/09/2026
19:09