

Dia do Cliente acende alerta para golpes com Pix e inteligência artificial



Com a proximidade do Dia do Cliente, celebrado em 15 de setembro, consumidores que pretendem aproveitar promoções e realizar compras pela internet devem redobrar os cuidados com a segurança financeira. O aumento das transações digitais também abre espaço para uma maior atuação de criminosos, que utilizam técnicas de engenharia social e recursos tecnológicos cada vez mais sofisticados para aplicar golpes.

Entre as principais ameaças estão fraudes envolvendo o Pix, falsos atendimentos bancários, ofertas fraudulentas, QR Codes adulterados e abordagens realizadas por aplicativos de mensagens. O avanço da inteligência artificial acrescentou ainda uma nova camada de preocupação, permitindo a criação de conteúdos capazes de imitar com precisão a voz e a imagem de pessoas conhecidas.

Inteligência artificial amplia sofisticação dos golpes

Ferramentas de inteligência artificial já são utilizadas por criminosos para produzir deepfakes, clonar vozes e reproduzir características de comunicação de familiares, amigos, funcionários de bancos e até autoridades.

Na prática, o golpista pode entrar em contato com a vítima simulando ser alguém de confiança e criar uma situação de urgência para induzi-la a realizar uma transferência.

Por isso, especialistas recomendam que o consumidor não considere apenas a voz, a fotografia ou a aparência de quem está entrando em contato como prova de identidade. Em situações envolvendo dinheiro, a orientação é confirmar a informação por outro canal de comunicação antes de realizar qualquer pagamento.

Conheça os golpes mais comuns

Durante períodos de maior movimentação comercial, como o Dia do Cliente, alguns tipos de fraude tendem a ganhar força. Entre os principais estão:

Falso funcionário de banco: criminosos entram em contato por telefone ou mensagem e se passam por funcionários de instituições financeiras para solicitar dados, códigos, senhas ou supostas confirmações de transações.

Golpe do Pix enviado por engano: o criminoso afirma ter realizado uma transferência equivocada e solicita a devolução do dinheiro, muitas vezes indicando uma conta diferente daquela que originalmente realizou o pagamento.

Falsas ofertas e QR Codes adulterados: anúncios divulgados em redes sociais podem direcionar o consumidor para páginas falsas, clonadas ou destinadas a receber pagamentos em contas de terceiros.

Golpe do falso parente: mensagens enviadas por aplicativos de comunicação simulam familiares ou amigos e alegam situações emergenciais para pressionar a vítima a realizar uma transferência imediata.

Caí em um golpe. O que fazer?

Em caso de fraude envolvendo o Pix, a rapidez pode ser decisiva. A primeira providência deve ser entrar em contato imediatamente com o banco e informar que a transação ocorreu em decorrência de fraude, solicitando a abertura do Mecanismo Especial de Devolução (MED).

Criado pelo Banco Central, o mecanismo permite que instituições financeiras adotem procedimentos para tentar bloquear e recuperar valores relacionados a determinadas situações de fraude envolvendo o Pix. Entretanto, o acionamento do MED não significa que a devolução do dinheiro esteja garantida, já que a recuperação depende da análise do caso e da disponibilidade dos recursos na conta que recebeu o valor.

Também é recomendável registrar um Boletim de Ocorrência e preservar todas as evidências relacionadas ao golpe.

Entre os documentos e informações que devem ser guardados estão:

comprovante da transferência;

capturas de tela das conversas;

números de telefone utilizados pelos criminosos;

e-mails recebidos;

links de anúncios ou páginas fraudulentas;

informações sobre a conta que recebeu o dinheiro;

protocolos de atendimento fornecidos pelo banco.

Esses registros podem ser importantes tanto para a investigação policial quanto para eventual contestação administrativa ou judicial.

Banco pode ser responsabilizado?

A responsabilidade das instituições financeiras em casos de golpes praticados mediante transferências realizadas pela própria vítima depende das circunstâncias de cada ocorrência.

É necessário avaliar, entre outros fatores, se houve falha na segurança ou na prestação do serviço bancário, se a instituição adotou mecanismos adequados de prevenção e monitoramento e quais medidas foram tomadas depois que a fraude foi comunicada.

Dessa forma, não existe uma regra que determine a devolução automática de todo valor perdido em um golpe. Cada situação precisa ser analisada individualmente.

Prevenção continua sendo a principal proteção

Antes de realizar uma transferência ou pagamento, o consumidor deve conferir cuidadosamente o nome do destinatário, o valor e os dados da operação.

Também é importante nunca compartilhar senhas, códigos de autenticação ou informações bancárias com terceiros. Links recebidos por mensagens, ofertas com preços muito abaixo do mercado e pedidos urgentes de transferência devem ser tratados com desconfiança.

Outra medida importante é manter aplicativos, sistemas operacionais e dispositivos atualizados, além de utilizar os mecanismos de autenticação e segurança disponibilizados pelas instituições financeiras.

No ambiente digital, a principal recomendação é simples: desconfie da urgência, confirme a identidade e pense antes de transferir.

Com golpes cada vez mais sofisticados e o uso crescente da inteligência artificial pelos criminosos, a segurança digital deixou de ser apenas uma preocupação tecnológica e passou a fazer parte da rotina financeira de qualquer consumidor.

Foto: Divulgação

<https://jornalpanfletus.com.br.cp3.masterix.inf.br/noticia/8804/dia-do-cliente-acende-alerta-para-golpes-com-pix-e-inteligencia-artificial> em 19/09/2026 09:44