RUFANDO BOMB NEWS Notícias sem rodeios

Sexta-Feira, 06 de Novembro de 2026

Fraudes Bancárias: Conheça os Principais Golpes e Aprenda a se Proteger

Fraudes digitais crescem 220%. Descubra as modalidades mais comuns e as melhores práticas de segurança para proteger sua conta.

As fraudes bancárias registraram um aumento alarmante de 220% no primeiro semestre do ano anterior, conforme dados revelados pela BioCatch. A modernização do sistema financeiro trouxe comodidade indiscutível, mas também criou oportunidades para esquemas criminosos cada vez mais refinados e sofisticados.

A incorporação de Inteligência Artificial nos ataques cibernéticos amplifica a sofisticação das fraudes, permitindo que criminosos criem imitações de vozes e contextos autênticos para enganar suas vítimas. Essa realidade exige uma abordagem integrada de proteção, combinando comportamentos seguros dos clientes com sistemas robustos nas instituições financeiras.

Modalidades de Golpe Mais Frequentes

A maioria das fraudes contemporâneas não explora brechas técnicas nos sistemas bancários, mas sim a vulnerabilidade psicológica do usuário. As principais formas incluem:

Falsa Central de Atendimento

O golpista se apresenta como funcionário da instituição, utilizando tecnologia para falsificar o número de telefone no identificador de chamadas. O criminoso simula situações urgentes como transações não autorizadas ou invasão de conta, pressionando a vítima para revelar senhas, códigos de segurança ou instalar programas de acesso remoto que concedem controle total do dispositivo.

Fraudes no Universo Pix

A velocidade do Pix torna-o alvo prioritário de criminosos. No esquema do Pix incorreto, o fraudador simula uma transferência acidental para o beneficiário e solicita devolução, fazendo com que a vítima devolva valores pessoais enquanto o golpista cancela sua transação original. Outra variante é o golpe do cartão para inadimplentes, onde promessas de altos limites por WhatsApp resultam em pagamentos de taxas fictícias.

Boletos Fraudulentos

Criminosos interceptam mensagens ou criam réplicas de portais legítimos para gerar boletos que aparentam autenticidade. Ao efetuar o pagamento, o recurso é transferido para a conta do defraudador ao invés do beneficiário legítimo.

Mecanismos de Proteção Implementados

A segurança funciona como responsabilidade conjunta entre a instituição e seu cliente. As defesas principais incluem autenticação biométrica facial para transações de valores elevados, bloqueio de acesso em novos aparelhos e o Mecanismo Especial de Devolução (MED), regulamentado pelo Banco Central para recuperação de valores em fraudes Pix quando notificado rapidamente. Certificações de conformidade em segurança também atestam o rigor dos procedimentos internos.

Orientações Essenciais de Proteção

Para garantir a integridade de sua conta, observe as seguintes diretrizes: institutos financeiros legítimos nunca solicitam senhas ou transferências para contas de validação; nunca instale programas de acesso remoto conforme orientação de chamadas telefônicas; sempre verifique o beneficiário e CNPJ antes de confirmar pagamentos de boletos; mantenha ceticismo em relação a mensagens que exigem ações imediatas.

Dúvidas Frequentes

A instituição realiza ligações para solicitar atualizações? Não. As atualizações ocorrem exclusivamente pelas plataformas oficiais de distribuição de aplicativos. Links para download via mensagens de texto ou WhatsApp são indicadores de fraude.

Qual é o procedimento em caso de transferência não autorizada via Pix? Comunique imediatamente ao banco através de canais autenticados para registrar uma contestação no MED. A celeridade aumenta as perspectivas de reembolso.

Como validar a autenticidade de um boleto? Confirme as informações do cedente no momento da transação. Serviços de atendimento estão disponíveis para esclarecer dúvidas sobre a legitimidade de documentos de cobrança.

O que caracteriza o esquema da falsa central? Trata-se de uma tentativa de roubo de informações confidenciais onde o criminoso simula ser representante da instituição. Instituições sérias nunca solicitam credenciais ou transferências por telefone.