


Transações NFC

Como as Instituições Financeiras protegem seus clientes no ambiente digital



Dileide de Abreu




Fundamentos da Segurança em Transações NFC

As transações NFC têm se tornado cada vez mais populares no setor financeiro devido à sua conveniência. Essa tecnologia permite que os clientes realizem pagamentos aproximando seus cartões ou dispositivos móveis de um terminal de pagamento. No entanto, a popularidade das transações NFC também atraiu a atenção de fraudadores. Assim, é crucial que as instituições financeiras implementem medidas eficazes de segurança.



1.1 Importância das Auditorias

É recomendável que as instituições financeiras realizem auditorias regulares em seus sistemas de segurança. Estas auditorias ajudam a identificar vulnerabilidades e implantar melhorias contínuas. O caso de uma instituição que sofreu uma violação de dados devido à falta de atualizações de segurança ilustra a importância dessa prática.

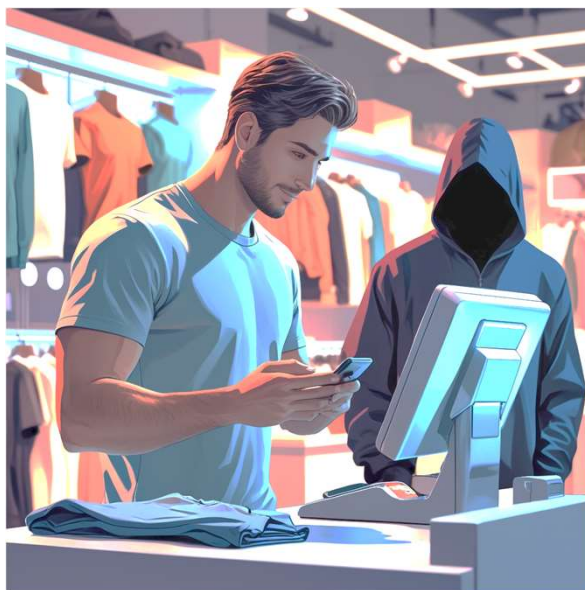



1.2 Ferramentas de Proteção de Dados

A criptografia é uma ferramenta essencial para proteger os dados durante as transações. Quando as informações estão criptografadas, mesmo que sejam interceptadas, não poderão ser lidas ou utilizadas. Instituições que implementaram, em sua conexão de internet, endereçamento IPv6 ou, em sua comunicação de dados, a tokenização, fornecem segurança adicional e são exemplos de práticas que podem mitigar esses riscos.

1.3 Riscos de Clonagem de Cartões

Um dos principais desafios na segurança das transações NFC é o risco de clonagem de cartões. Um exemplo é a instalação ilegal de dispositivos, os chamados skimming, em caixas eletrônicos ou terminais de ponto de venda. Através deles, fraudadores copiam as informações dos cartões. Esses dados são, então, utilizados para realizar compras fraudulentas, causando prejuízos significativos tanto para os consumidores quanto para as instituições.





Métodos de Autenticação e Monitoramento

A autenticação forte é uma necessidade para aumentar a segurança nas transações NFC. Ao combinar senhas com métodos biométricos, como impressão digital, as instituições podem garantir que apenas usuários autorizados realizem pagamentos. Um exemplo de falha nessa área é o phishing, quando um fraudador leva usuários desavisados a compartilhar informações de autenticação.



2.1 Alertas em Tempo Real

É fundamental que as instituições implementem alertas em tempo real para informar os clientes sobre transações realizadas. Isso permite que os clientes identifiquem e relatem imediatamente atividades suspeitas. Um exemplo prático é o envio de sms, após cada uso do cartão. Assim, vários usuários podem ser notificados sobre compras não autorizadas, resultando no rápido bloqueio de seus cartões.


2.2 Estabelecimento de Limites de Transação

As instituições financeiras devem estabelecer limites de transação para pagamentos NFC. Essa medida limita o impacto de eventuais fraudes, a fim de proteger o cliente e a própria instituição. Um exemplo foi o caso de clientes que tiveram o limite de transação diário reduzido após tentativas de uso irregular, o que ajudou a evitar perdas financeiras.



2.3 Monitoramento em Tempo Real

O monitoramento em tempo real das transações também desempenha um papel vital na prevenção de fraudes. Sistemas de inteligência artificial estão sendo utilizados para analisar padrões de comportamento e detectar transações anômalas. Desta maneira, a área de segurança de um banco consegue evitar uma série de transações fraudulentas a partir de, por exemplo, um cartão que estava sendo usado em locais geograficamente distantes em um curto período de tempo.



Educação do Cliente e Boas Práticas

Educar os clientes sobre as boas práticas de segurança é essencial para mitigar riscos. As instituições financeiras devem fornecer informações claras sobre o uso seguro de cartões e dispositivos móveis. Casos como o de clientes que ignoraram avisos de segurança e acabaram caindo em fraudes mostram como a falta de conhecimento pode resultar em perdas financeiras.



3.1 Aplicativos de Gerenciamento de Transações

Uma prática recomendada envolve o uso de aplicativos que permitem o gerenciamento e monitoramento de transações. Com esses aplicativos, os clientes podem verificar movimentações em tempo real, aumentando a conscientização. Em uma consulta online rápida, o próprio cliente pode se dar conta de um incidente notório e conseguir impedir a transação suspeita, através de um simples comando de não reconhecimento da mesma, resultando em uma rápida ação corretiva.


3.2 Opção de Desativação do NFC

As instituições devem oferecer a opção de desativar a funcionalidade NFC em cartões quando não estiver em uso. Essa prática é útil, especialmente em situações nas quais os usuários estejam em ambientes de alto risco. Um usuário de cartão pode vir a desativar o NFC numa situação de uma festa de rua, evitando assim o possível golpe por aproximação de uma maquininha/terminal de compra, no meio da multidão, por parte de um golpista.

3.3 Fomentando Hábitos de Segurança

Por último, fomentar hábitos de segurança entre os clientes tem impactos diretos e positivos na redução de fraudes. Ao incentivar a verificação regular de extratos e a denúncia imediata de atividades suspeitas, instituições financeiras contribuem para um ambiente mais seguro. O caso de uma cliente que notificou seu banco rapidamente, evitando assim uma série de transações fraudulentas, sublinha a importância dessa colaboração entre instituições financeiras e clientes.





Obrigada por conhecer mais sobre esse importante tema!

Esse e-book foi gerado por IA e diagramado por humano.

AUTORA:

Dileide de Abreu

dileide.moreira@caixa.gov.br