Toque Fantasma: O medo invisível nas transações por aproximação

Algo assustador está acontecendo no universo dos pagamentos digitais. O simples toque por aproximação, que antes era sinônimo de praticidade e segurança, agora virou uma preocupação de arrepiar a espinha: o “toque fantasma”. A expressão, que poderia remeter a histórias de terror, define o medo real que muitos consumidores começaram a sentir diante de uma fraude capaz de agir sem deixar rastros visíveis. É um lembrete inquietante de que, na era da hiperconectividade, até os gestos mais simples podem esconder armadilhas sofisticadas.

Uma investigação recente da Kaspersky revelou que essa modalidade de golpe está se espalhando com rapidez. O esquema utiliza aplicativos maliciosos para interceptar o token (código temporário gerado em pagamentos por aproximação - NFC) e retransmiti-lo em tempo real para outro aparelho, que conclui uma compra fraudulenta como se fosse o cartão original da vítima. Em números, o Brasil lidera o ranking global de tentativas bloqueadas, respondendo por 47% dos casos detectados no mundo. Um dado alarmante que reforça o quanto nosso ecossistema digital, embora avançado, ainda é terreno fértil para a ação de cibercriminosos criativos.

O golpe se desdobra em duas frentes, presencial e virtual, ambas igualmente engenhosas. Na versão presencial, o cenário é cotidiano: um café, uma fila, um show. Em segundos, um criminoso se aproxima da vítima com o celular e captura o token do pagamento NFC do cartão ou smartphone. Esse código é imediatamente transmitido para o aparelho de um comparsa, que o utiliza em uma maquininha para concluir uma transação legítima, porém indevida. Tudo acontece tão rápido que a vítima dificilmente percebe o “toque” que roubou seu saldo.

A modalidade virtual, no entanto, é ainda mais perigosa. Ela troca a agilidade das ruas pela sutileza da manipulação. Aqui, o golpe começa com engenharia social: um criminoso se passa por um atendente de banco ou empresa de cartão e orienta a vítima a instalar um aplicativo para “verificar” o cartão. Esse aplicativo, claro, é falso. Ao aproximar o cartão do celular para supostamente validá-lo, o usuário permite que o app capture o token NFC e o retransmita para o aparelho do golpista,

que finaliza a compra remotamente. Nesse caso, soluções de segurança com assinatura digital de código (Code Signing), como as oferecidas pela GlobalSign, poderiam mitigar o risco, já que atestam a autenticidade do desenvolvedor.

Assustador, mas evitável

O “Toque Fantasma” é um lembrete contundente de que a segurança digital não se resume a senhas fortes ou a dispositivos modernos. Ela depende de uma combinação de tecnologia confiável, atenção contínua e educação digital. No mundo físico, manter distância de desconhecidos e proteger seus cartões continua sendo prudente. Já no mundo virtual, é essencial evitar o download de aplicativos fora das lojas oficiais e desconfiar de qualquer contato não solicitado pedindo a instalação ou validação de dados.

Hoje em dia, o medo não vem mais de portas que abrem sozinhas, mas de cliques que parecem inofensivos. Quando a fraude se disfarça de conveniência, o antídoto é composto por informação, cautela e soluções tecnológicas robustas. O verdadeiro “fantasma” é a desatenção, e combatê-lo requer atenção constante e hábitos digitais cuidadosos.

SOBRE LUIZA DIAS

Luiza Dias é Presidente da GlobalSign Brasil - empresa líder no mercado de certificação digital no mundo. Vencedora da categoria ‘Melhor CEO’ do Open Mind Awards 2024, Luiza é a única mulher latino-americana a ocupar este cargo em uma Autoridade Certificadora (AC) de Raiz Internacional. Possui 19 anos de carreira, 10 deles dedicados à GlobalSign, onde ocupou os cargos de Vendedora, Gerente de Vendas Latam e, desde 2021, a presidência para o Brasil. Foi responsável por implantar o primeiro escritório físico da empresa no país, localizado em Belo Horizonte (MG), e tornou-se uma importante referência feminina do mercado de tecnologia e cibersegurança de toda a América Latina.