TEXTO DE ATUALIDADES
PRINCIPAL DE MATEMÁTICA+TESTE 01
8º E 9º ANO - IIIª UNIDADE

Pix cresce, e número de fraudes também

Pix alcança novo recorde de transações em um único dia, mas golpes e fraudes ainda são desafios para maior segurança dos usuários.

Danielle Ruas 11 Min Leitura Abril 11, 2024

No dia 5 de abril, o Pix atingiu um novo recorde com mais de **200 milhões de transações realizadas em apenas 24 horas**. Na data, foram contabilizadas 201,6 milhões de transferências via Pix para usuários finais. E a alta demanda gerou instabilidade no funcionamento do sistema.

O recorde anterior era de 178,686 milhões de transações em um único dia. Esse marco ocorreu em 7 de março. Já no sábado (6/4), o sistema de pagamento Pix registrou um total de 171,4 milhões de transações, estabelecendo um novo patamar para esse dia da semana.

Apesar do **Banco Central** garantir a estabilidade de seus sistemas, vários clientes de bancos e instituições financeiras enfrentaram problemas ao longo do dia.

Pix, o queridinho dos consumidores

Consoante os dados do **Banco Central**, desde seu lançamento em novembro de 2020, o Pix acumulou 161,99 milhões de usuários até o final de março, sendo 147,95 milhões de pessoas físicas e 14,04 milhões de pessoas jurídicas. Em fevereiro, o sistema alcançou a marca de movimentação de mais de R$ 1,71 trilhão.

Se de um lado há o alto volume em número de pessoas e transações financeiras, do outro existe o recorrente aumento de fraudes, o que acarreta graves prejuízos aos consumidores. Para agravar ainda mais o cenário, não são poucos os consumidores que, ao registrar reclamação, são surpreendidos com a recusa ou omissão dos bancos e instituições financeiras na tratativa das suas dores. E ao passo que o sistema de pagamento instantâneo vai crescendo, os golpes e fraudes vão ficando também cada vez mais bem elaborados.

O mais novo golpe do Pix

O mais recente, inclusive, foi divulgado recentemente pela **Kaspersky, especialista em proteção online avançada**. O golpe é realizado sem a necessidade de invadir computadores ou celulares com vírus, o que exige maior atenção dos consumidores. Em nota, a empresa explicou que os cibercriminosos, para aplicar o golpe, estão utilizando a ferramenta Reboleto, a qual possibilita o monitoramento de e-mails com anexos. Dessa forma, eles conseguem buscar palavras-chave como "Pix", "boleto", "pagamento de conta" e outras relacionadas. Os golpistas conseguem, então, editar QR Codes e código de barras nas faturas, mesmo em e-mails não lidos pela vítima.

As intervenções realizadas pelos golpistas nos e-mails não requerem vírus. E todo valor é redirecionado para contas de laranjas. Isso exige dos consumidores atenção redobrada na verificação das informações do destinatário antes de efetuar pagamentos. Vale ressaltar que as mudanças têm sido feitas não apenas em e-mails, mas também quando os dados são gerados pelo consumidor em sites e aplicativos de empresas durante o pagamento. Vale ressaltar que o QR Code ou código de barras gerado não garante a segurança das operações financeiras pelo PIX, sendo essencial que o consumidor verifique os dados do favorecido antes de finalizar a transação.

Prevenção no Pix

"Para usar o PIX de forma preventiva, é essencial confirmar o destinatário do QR Code antes de realizar qualquer pagamento ou transferência bancária", aconselha **Armindo Sgorlon, CEO da SGA, empresa do grupo FCamara**, atuante nas áreas de cloud, cibersegurança e data & analytics.

Em caso de problema, é necessário registrar imediatamente o ocorrido com o banco, a empresa envolvida e também o Banco Central, guardando os números de protocolo para caso surjam possíveis controversas. Se o problema persistir, é recomendável buscar ação judicial para a devolução do valor enviado via Pix, juntamente com possíveis danos morais comprovados pelo golpe.

Neste aspecto, vale salientar que a tese do **Tema Repetitivo 466 e a Súmula 479 do Superior Tribunal de Justiça**, as instituições bancárias são sim objetivamente responsáveis por danos causados por fraudes praticadas por terceiros, devido ao risco da atividade. Ademais, as empresas também são responsáveis perante o consumidor ao permitir falhas em seus sistemas e ação de terceiros estelionatários, conforme previsto nos artigos 12 a 14 do **Código de Defesa e Proteção do Consumidor (CDC)**.

Dados bancários

O Tema Repetitivo e a Súmula, publicado no Diário de Justiça em 9 de outubro de 2023, expõem que os dados sobre operações bancárias são, em regra, de tratamento

exclusivo pelas instituições financeiras. No ponto, a **Lei Complementar n.º 105/2001** estabelece que as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados (art. 1º), constituindo dever jurídico dessas entidades não revelar informações que venham a obter em razão de sua atividade profissional, salvo em situações excepcionais. Desse modo, seu armazenamento inadequado, a possibilitar que terceiros tenham conhecimento de informações sigilosas e causem prejuízos ao consumidor, configura defeito na prestação do serviço (**art. 14 do CDC e art. 44 da Lei Geral de Proteção de Dados**).

A jurisprudência ainda vem de encontro com os princípios como o da confiança e a função social do contrato. Assim, o contrato de consumo é mais do que um instrumento jurídico, e sim um meio para proteger os interesses legítimos do consumidor.

Ataques cibernéticos no Brasil

O Brasil encontra-se atualmente na segunda posição no ranking dos países mais vulneráveis a ataques cibernéticos no mundo, sofrendo 45,9 bilhões de investidas apenas no primeiro semestre de 2022. Os dados são da **empresa de cibersegurança Trend Micro**. Ao analisar os recordes do Pix da última semana, **Armindo Sgorlon, CEO da SGA**, destaca que durante períodos de grande movimentação, o e-commerce torna-se um alvo extremamente atrativo para ataques e tentativas de golpe. “Nesse aspecto, é essencial que as empresas estejam equipadas com boas soluções de cibersegurança e que os clientes saibam identificar sinais de fraude”.O executivo aponta outros dois pontos cruciais para os consumidores que compram online.

Phishing

Phishing (pronuncia-se fishing): alguém que executa um phishing “morde o anzol” lançado pelo phisher. Ou seja: os criminosos utilizam esta técnica para “pescar” os dados das vítimas, como senha ou número de cartão. Para “pescar” a vítima, os golpistas geralmente se passam por funcionários de uma organização confiável e enviam um SMS, WhatsApp ou e-mail com um link. Os criminosos podem obter dados de login e senha, por exemplo, se a pessoa cair na armadilha e clicar, direcionando-a para um site falso.

“Outra forma desse golpe acontecer é quando a pessoa recebe uma mensagem informando que foi contemplada com um cupom de desconto e, para utilizá-lo, é seu dever preencher os dados. Por isso, é importante sempre desconfiar de links suspeitos que aparecem aleatoriamente em e-mails ou mensagens, questionar o nome do remetente e, é claro, desconfiar também de promoções exageradas”, explica Armindo.

Selos de segurança

Selos e certificados de segurança: lojas virtuais usam esse tipo de recurso para proteger os dados dos usuários e o site em si contra fraudes.

Ao acessar uma loja online, é fundamental verificar a presença do cadeado ao lado da URL do site e também selos de segurança no rodapé da página, pois esses detalhes indicam que a conexão é segura.

“Realizar compras online pode e deve ser uma experiência tranquila e positiva para o consumidor, sem que ele precise se preocupar com a proteção de suas informações

ou com possíveis golpes. Sgorlon pontua que os comerciantes também devem garantir a segurança cibernética de ponta a ponta em seus negócios. “Eles são o alvo do alerta”.

Ruas, Danielle. Pix cresce, e número de fraudes também. C**onsumidor Moderno**. São Paulo, 2024. Disponível em: < https://consumidormoderno.com.br/pix-crescimento-fraudes/ >. Acesso em: 15 de julho de 2024