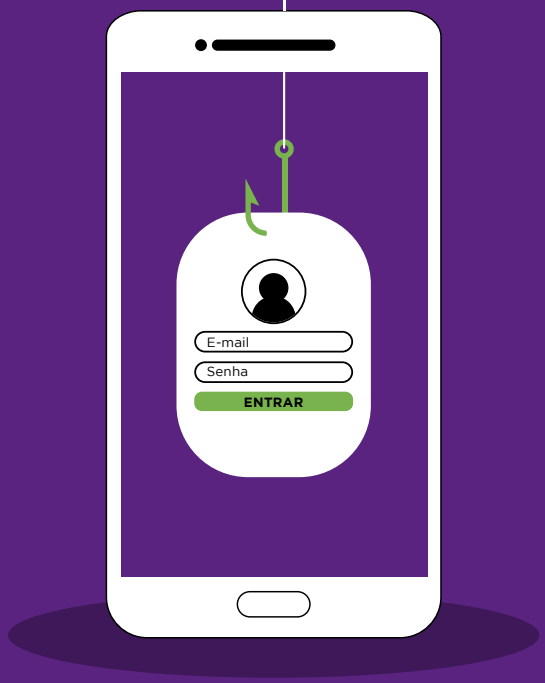
GuiaDosBancos
Responsáveis

GOLPE DO CELULAR INVADIDO: A RESPONSABILIDADE DOS BANCOS E O DIREITO DOS CONSUMIDORES



REALIZAÇÃO

idec
Instituto Brasileiro de Defesa do Consumidor

APOIO

Sida

FICHA TÉCNICA

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR – IDEC

INSTITUCIONAL

DIRETORIA EXECUTIVA

Carlota Aquino

Igor Rodrigues Britto

GERÊNCIA DE PROGRAMAS E PROJETOS

Georgia Carapetkov

AUTORIA

Fábio Machado Pasin

Ione Alves Amorim

REVISÃO

Ione Alves Amorim

Anderson Resende

Christian Printes

PROJETO GRÁFICO E CAPA

Renata Castro Fagundes

ASSESSORIA DE IMPRENSA

Daniel Torres

Ohana Oliveira

Fernando Gentil

CONTRIBUIÇÕES

Fernando Gentil

Luã Cruz

Lucas Marcon

APOIO

SIDA - Agência Sueca de Cooperação para o Desenvolvimento Internacional

Oxfam Novib

SOBRE O IDEC:

O Idec (Instituto Brasileiro de Defesa do Consumidor) é uma organização da sociedade civil brasileira criada em 1986 com o objetivo de defender os direitos do consumidor, incluindo os direitos dos usuários de serviços públicos, a luta por relações econômicas justas e equilibradas e a ampliação do acesso a bens e serviços essenciais. O Idec é uma associação de consumidores que atua em completa independência de governos, empresas e partidos políticos.

SOBRE O GBR:

O GBR (Guia dos Bancos Responsáveis) é um projeto da Fair Finance International que avalia as políticas dos nove principais bancos brasileiros em diferentes temas, como a defesa do consumidor, meio ambiente, direitos humanos e outros. Ele é formado por uma coalizão que fazem parte o Idec, o Instituto Sou da Paz, a Conectas Direitos Humanos, a Oxfam Brasil e a Proteção Animal Mundial.

SUMÁRIO

RESUMO

Este trabalho buscou levantar as medidas de segurança que vinham sendo adotadas pelo Nubank, Itaú, Bradesco e Santander para prevenir e reparar perdas de consumidores vítimas de uma nova modalidade de golpe financeiro realizada com a utilização de aplicativos de acesso remoto, também conhecido como golpe da mão fantasma, golpe do acesso remoto ou **golpe do celular invadido**.

Um aplicativo de acesso remoto é um software que permite que um dispositivo, como um computador ou smartphone, seja controlado e acessado remotamente por outra pessoa, que se utiliza de outro dispositivo conectado à internet. Isso possibilita a visualização e operação do dispositivo como se estivesse fisicamente presente no local onde ele está localizado.

O documento foi motivado pela constatação inicial do aumento de reclamações de clientes do Nubank e a repercussão nas redes sociais. Os quatro bancos foram notificados pelo Instituto Brasileiro de Defesa do Consumidor para esclarecer as medidas adotadas contra esses golpes.

O conteúdo de suas respostas variaram, mas todos afirmaram investir em segurança e conscientização dos clientes. Porém, a resposta do banco Itaú se destacou por afirmar que o banco possuiria mecanismo de segurança específico capaz de bloquear transações feitas via aplicativo de acesso remoto. O trabalho buscou analisar as informações fornecidas pelos bancos, realizar testes de transações via acesso remoto dos aplicativos bancários das quatro instituições financeiras destacadas e fornecer orientações aos consumidores afetados.

Sobre os testes, não se busca atingir um nível de rigor científico nos resultados obtidos por meio deles. Evita-se a utilização do termo “estudo”, preferindo-se a denominação de teste. Entretanto, os resultados indicam claramente a presença de falhas nos sistemas de segurança de alguns aplicativos bancários no contexto brasileiro.

O teste de segurança não tem a intenção de se configurar como uma pesquisa científica estrita. Não se almeja afirmar que os resultados do teste refletem a situação ampla sobre

segurança dos aplicativos bancários. O propósito subjacente aos testes de segurança é conduzir uma avaliação que possua objetivos instrutivos e de relevância política. Aqui, também deseja-se conscientizar as pessoas consumidoras para que tenham uma melhor percepção sobre a integridade dos dados em uma tecnologia do cotidiano e compreendam as vulnerabilidades dos aplicativos, incitando a formação de uma "consciência jurídica" e uma compreensão mais profunda das questões de segurança cibernética.

Além disso, buscou-se discutir a transparência e responsabilidade dos bancos, apresentando os direitos dos consumidores e argumentando pela **obrigação do ressarcimento por parte das instituições financeiras**. Os resultados do trabalho também poderão ser usados para subsidiar o regulador e promover diálogos institucionais.

01
INTRODUÇÃO

Em 5 de abril de 2023, o Nubank emitiu um alerta por e-mail para seus clientes sobre o golpe do celular invadido. No informe, o banco alertou que esta modalidade de golpe ocorreria devido ao download, pelo cliente, de aplicativo ilegítimo capaz de permitir ao fraudador o acesso remoto do celular do consumidor. Há variações de como o golpe é operacionalizado, mas, segundo relatos de consumidores, sua forma mais comum seria a partir do uso de técnicas de engenharia social associadas a falha de segurança dos aplicativos bancários.

As vítimas seriam contatadas por um falso operador da central de atendimento do banco, informando que haveria sido identificada uma tentativa de golpe e, com isso, o operador induziria o consumidor a instalar um aplicativo de acesso remoto. Ao instalar o aplicativo, o fraudador visualizaria a tela do dispositivo móvel do consumidor e instruiria o consumidor a acessar seu aplicativo bancário. Por monitorar todos os passos do consumidor, o fraudador seria capaz de identificar a senha de acesso digitada pela vítima. Além disso, por estar acessando o dispositivo celular de maneira remota, poderia manusear o aplicativo bancário livremente.

Nesse período, o Idec tomou conhecimento de um aumento significativo nas reclamações de clientes do Nubank relacionadas ao golpe. A equipe de Comunicação do Idec, durante monitoramento de redes, constatou que o assunto ocupou *trending topics* de redes sociais como o Twitter.

Diante desse contexto, em 6 de abril de 2023, a equipe de Serviços Financeiros enviou uma notificação ao banco com o objetivo de esclarecer quais providências estariam sendo adotadas pela instituição financeira para proteger e ressarcir seus clientes. Em sua notificação, o Idec alegou que, em conformidade com a Teoria do Risco da Atividade, seria responsabilidade do banco prever essa vulnerabilidade e fornecer mecanismos de segurança para evitar as fraudes relatadas.

Após a resposta do Nubank e, realizado novo levantamento da equipe de Serviços Financeiros do Idec, também se identificou a publicação de posicionamentos institucionais

a respeito do golpe do celular invadido por parte do Banco Itaú, Bradesco e Santander. Dessa forma, em 28 de abril de 2023, essas instituições financeiras também foram notificadas. Nessa notificação, solicitou-se esclarecimentos sobre as medidas adotadas para prevenir e remediar os consumidores vítimas desse golpe. O objetivo também foi verificar se alguma dessas instituições possuiria mecanismos de segurança mais eficazes para prevenir o golpe do acesso remoto.

Suscitou-se assim um debate sobre a responsabilidade dos bancos diante de golpes e fraudes realizados mediante uso de ferramentas tecnológicas associadas ao uso de técnicas de engenharia social. Dessa maneira, **o primeiro objetivo** do presente relatório foi **analisar e relatar as informações apresentadas pelos bancos**. Como **segundo objetivo**, buscou-se **testar os aplicativos dos quatro bancos** mencionados com a finalidade de verificar se seria possível acessar o aplicativo dos bancos e realizar uma transação bancária a partir da utilização de software de acesso remoto.

Buscou-se também apresentar para os consumidores seus respectivos direitos diante de situações envolvendo golpes financeiros, apoiando-se em teses que demonstram **a obrigatoriedade do ressarcimento por parte das instituições financeiras**. Por fim, também se objetivou subsidiar o regulador sobre a questão, buscando-se diálogos institucionais a partir dos resultados do trabalho.

02
RESPOSTAS DAS INSTITUIÇÕES FINANCEIRAS

2.1. NUBANK

Em 06 de abril, o Idec notificou o Nubank, informando que os correntistas do banco estariam sendo vítimas da modalidade de fraude conhecida como Golpe do Acesso Remoto. Nessa modalidade, o fraudador induz o consumidor a instalar um aplicativo que permite que um dispositivo, como um computador ou smartphone, seja controlado e acessado remotamente por outra pessoa, que se utiliza de outro dispositivo conectado à internet. Isso possibilitaria ao fraudador a visualização e operação do dispositivo do consumidor como se estivesse fisicamente presente no local onde ele está localizado. Dessa forma, o aplicativo bancário do cliente permitiria ao fraudador realizar transações bancárias de maneira remota, sem a necessidade de utilização de cartão físico ou senhas do cliente.

A notificação foi acompanhada de denúncias que indicavam que o sistema de segurança do banco não estaria coibindo adequadamente tais transações, permitindo que os fraudadores realizassem operações bancárias não autorizadas.

Em sua notificação, o Idec alegou que, de acordo com a Teoria do Risco da Atividade, é responsabilidade do banco prever e evitar eventuais vulnerabilidades dos sistemas digitais, fornecendo aos clientes um aplicativo seguro para prevenir esse tipo de golpe. Além disso, o Instituto destacou que o Nubank deveria agir prontamente para atender as demandas dos consumidores vítimas dessa fraude, **reparando os danos causados e ressarcindo os valores indevidamente retirados das contas**.

O Idec baseou-se no **artigo 14 do Código de Defesa do Consumidor**, que estabelece que o **fornecedor de serviços é responsável por reparar os danos decorrentes de falhas na prestação de serviços**. Ainda, o Instituto destacou a **Súmula 479 do Superior Tribunal de Justiça**, que firmou o entendimento no sentido da **responsabilidade objetiva das instituições financeiras por danos causados por fraudes e delitos praticados por terceiros no contexto de operações bancárias**.

Para obter esclarecimentos sobre a situação, o Idec solicitou ao Nubank informações detalhadas sobre (i) as medidas que o banco estaria adotando para evitar tais fraudes, (ii) o

volume de casos já tratados relacionados a esse tipo de crime, bem como (iii) os procedimentos e prazos para atender e ressarcir os consumidores prejudicados. O prazo dado para as respostas foi de 15 dias corridos a partir da data de recebimento do comunicado por email.

Em resposta aos questionamentos, **o Nubank** afirmou, em 20 de abril, que não haveria falha de segurança atribuível ao banco, argumentando que o *modus operandi* desse tipo de golpe envolveria engenharia social e, portanto, estaria além de seu poder de vigilância. Também informaram que o golpe ocorreria por meio do uso de aplicativos legítimos, como AnyDesk e TeamViewer, contradizendo seu alerta inicial, que orientava o consumidor, como sendo uma medida de segurança preventiva contra este golpe, a não baixar aplicativos de lojas não oficiais.

O Nubank também mencionou o Pack de Proteção e o SOS Nu como ferramentas de prevenção e segurança, que envolveriam sistemas de reconhecimento, autenticação e modelos preditivos para mitigar riscos e garantir a defesa contra ameaças externas. Além disso, o banco informou disponibilizar de canais de atendimento para que os clientes reportem os incidentes e acionem o Mecanismo Especial de Devolução (MED) em situações de suspeita de fraude para reaver valores evadidos via Pix.

Por fim, o banco afirmou que o problema afetava igualmente outros aplicativos bancários e citou publicações feitas em sites institucionais de outros bancos em operação no Brasil.

2.2. ITAÚ, BRADESCO E SANTANDER

Diante dessas alegações e, considerando o levantamento a respeito de publicação de instituições financeiras em seus sites institucionais, abordando medidas de segurança relacionadas ao golpe, o Idec, em 28 de abril de 2023, também notificou **os bancos Itaú, Bradesco e Santander**. Nesta notificação, em teor semelhante à enviada ao Nubank, solicitou-se esclarecimentos sobre as medidas adotadas para prevenir e remediar os consumidores vítimas desse golpe. O objetivo também foi verificar se alguma dessas instituições possuiria mecanismos de segurança mais eficazes para prevenir o golpe do celular invadido.

Em resposta apresentada em 12 de maio de 2023, o **Banco Itaú** informou que seus aplicativos bancários utilizados para acesso às contas **possuem mecanismos de segurança**

que buscam impedir o acesso remoto de terceiros, tais quais os descritos na notificação. Segundo o banco, o objetivo principal dessa proteção seria evitar que softwares conhecidos de mercado, que viabilizem acesso remoto, estejam em funcionamento quando o cliente abrir o aplicativo de acesso à conta corrente do Itaú.

O banco também afirmou que realiza comunicações e campanhas de prevenção a golpes e fraudes, não apenas para seus clientes, mas para toda a sociedade.

Sobre o uso de ferramentas de acesso remoto durante o uso do aplicativo, o Itaú destacou que seus sistemas são preparados para evitar esse tipo de acesso e que seus mecanismos são revisados e atualizados sempre que necessário. Segundo o banco, os sistemas de prevenção a fraudes incluem mecanismos de controle e monitoramento, como criptografias, senhas, reconhecimentos biométricos, autenticações por códigos, proteções para tentativas de acesso remoto ou robotizadas e monitoramento comportamental e transacional.

Por fim, o banco ressaltou que o detalhamento de suas medidas de segurança seria uma informação extremamente sensível e sua divulgação poderia comprometer sua eficácia, tornando os sistemas vulneráveis a fraudadores. Portanto, considera esse tema como confidencial e avalia com cautela a divulgação de informações adicionais.

Já o **Santander**, em 12 de maio de 2023, respondeu informando que investe em tecnologia da segurança e que trata com seriedade as reclamações de seus clientes. Também respondeu que a instituição investe, de maneira perene, nas áreas de tecnologia e segurança da informação. Além disso, alegaram realizar diversas ações de conscientização com seus respectivos clientes, buscando orientá-los da existência de golpes financeiros mais comuns e quais são as melhores práticas para se proteger.

Embora o banco tenha mencionado alguns investimentos em tecnologia e segurança da informação, **não forneceu detalhes específicos sobre as medidas concretas que adotou para evitar o acesso remoto não autorizado às contas dos clientes**.

A resposta mencionou ações de conscientização e disponibilidade da central de atendimento para acolher manifestações de ocorrências suspeitas, mas também não ofereceu informações detalhadas sobre os mecanismos específicos que estão sendo implementados ou aprimorados para prevenir e detectar tais golpes.

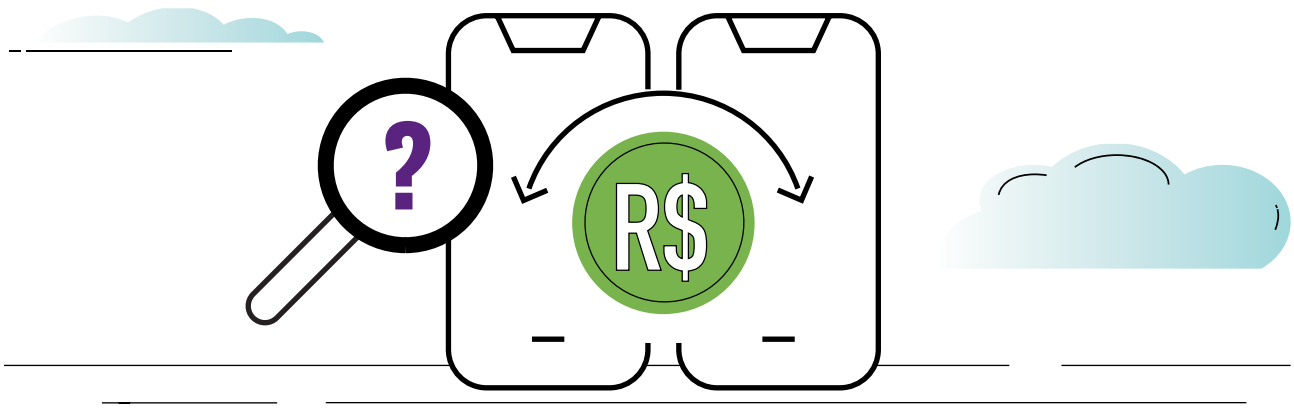
Uma resposta mais robusta teria incluído informações específicas sobre as tecnologias e protocolos específicos de prevenção do acesso remoto não autorizado, demonstrando o compromisso e a eficácia das ações do Santander em proteger seus clientes contra fraudes.

Por fim, o **Bradesco,** em 20 de junho de 2023, após o envio de duas notificações, informou que a segurança de seus clientes é uma prioridade para o banco, destacando que investem em tecnologia e possuem um ecossistema de prevenção à fraude regido por um motor de segurança. Esse motor de segurança utilizaria regras e modelos de transações para identificar movimentações atípicas dos clientes e mitigar o risco de fraudes. O banco também mencionou a existência de centrais de monitoramento que analisam transações de maior risco identificadas pelo motor de segurança.

Além disso, o Bradesco descreveu as formas de autenticação utilizadas para acessar seus canais (Internet Banking e Bradesco Celular) através de senhas e outros dispositivos de segurança.

O banco destacou também suas ações de conscientização, fornecendo orientações aos clientes sobre o uso seguro dos canais bancários, compartilhando dicas de segurança em seus canais de atendimento, redes sociais e site.

No entanto, apesar de o Bradesco mencionar que possui um ecossistema de prevenção à fraude com regras e modelos de transações, **não forneceu detalhes sobre como esse sistema funciona, quais são as regras específicas adotadas ou como é feita a análise de transações suspeitas**. Além disso, o banco mencionou analisar mais de 22 bilhões de transações anualmente para mitigar riscos, mas não forneceu informações sobre a taxa de sucesso na prevenção de fraudes, o número de fraudes detectadas e resolvidas, ou o número de clientes afetados por golpes.



03
RESPOSTA MODELO DO ITAÚ E ENVIO DE NOVA NOTIFICAÇÃO PARA NUBANK, SANTANDER E BRADESCO

Diante das respostas dos bancos enviadas em maio de 2023, o Itaú foi o único que alegou possuir medida de segurança específica para impedir tentativas de transações feitas via aplicativos de acesso remoto.

O fato de existir ferramenta de segurança disponível no mercado capaz de bloquear transações feitas via acesso remoto seria um indício da falha de segurança dos demais bancos que não haviam implementado tal medida até o referido período de maio de 2023. Com efeito, em 30 de maio, baseando-se na resposta do Itaú, o Idec apresentou nova notificação para os bancos Nubank, Santander e Bradesco, alegando a necessidade da adoção de medidas de segurança para evitar o golpe do celular invadido.

No novo documento enviado, o Idec afirmou reconhecer as iniciativas do Nubank, Santander e Bradesco, como investimentos em tecnologia de segurança, conscientização dos clientes e melhoria das políticas relacionadas a golpes financeiros. No entanto, destacou a importância de fortalecer ainda mais as medidas preventivas de segurança, como as alegadas pelo Itaú.

O Idec solicitou que as instituições financeiras avaliassem cuidadosamente as recomendações e informassem, em até 15 dias, as medidas adicionais que seriam tomadas em relação à segurança do acesso remoto em seu aplicativo bancário.

Em resposta ao Idec em 14 de junho, o **Nubank** enfatizou seu compromisso contínuo em aprimorar as medidas de segurança para prevenir golpes e fraudes. A empresa destacou que a proteção dos clientes é uma prioridade e que investem constantemente em tecnologia e ferramentas de segurança para garantir a integridade das operações e a proteção dos dados.

O Nubank mencionou que notifica os clientes sobre atualizações do aplicativo, assegurando que todas as camadas de segurança estejam em pleno funcionamento e os mecanismos de prevenção a fraudes estejam atualizados. Além disso, **informou que dispõe**

de mecanismos capazes de identificar e repelir ameaças, incluindo softwares de acesso remoto e malwares, garantindo a segurança dos clientes durante toda a jornada de utilização dos serviços.

Um ponto relevante abordado pelo Nubank foi a criação do "Canal de Denúncias", recém lançado para receber relatos de pessoas que tomaram conhecimento ou foram vítimas de tentativas de fraudes e golpes em que uma conta Nubank esteja envolvida. Esses relatos, segundo o banco, seriam essenciais para que a empresa adote medidas preventivas e impeça a ocorrência de novos incidentes ou tentativas de ameaças.

Por razões de sigilo, segurança e efetividade dos controles, o Nubank optou por não divulgar detalhes minuciosos sobre todos os mecanismos de segurança implementados, já que a exposição dessas informações poderia tornar o sistema vulnerável a fraudadores e pessoas mal intencionadas.

Finalizando a resposta, o Nubank reiterou seu compromisso em proporcionar a melhor experiência para seus clientes e reafirmou sua disponibilidade para qualquer esclarecimento ou necessidade adicional.

Em sua resposta, **o Nubank não afirmou explicitamente que conseguiria bloquear todas as transações feitas por acesso remoto. Porém, a empresa mencionou que dispunha de mecanismos capazes de identificar a tentativa de atuação de aplicativos de acesso remoto e de outros aplicativos maliciosos ("malwares") no dispositivo do cliente**. Essas ferramentas teriam o objetivo de repelir essas ameaças, atuando contra a ação de softwares que poderiam ser instalados no dispositivo pelos clientes e impedindo a execução de ações por um "dispositivo espelho" (dispositivo utilizado pelo fraudador, com acesso ao que é transmitido na tela do celular do cliente).

Embora o Nubank tenha mencionado medidas para identificar e repelir ameaças, **a resposta não fornece uma declaração direta e inequívoca de que todas as transações feitas por acesso remoto estão completamente bloqueadas**. O foco da resposta do Nubank foi ressaltar suas iniciativas de segurança, políticas de proteção ao cliente e ações de prevenção a fraudes, mas não especificou detalhes completos sobre a abrangência e eficácia de suas medidas de bloqueio de transações por acesso remoto.

Em 14 de junho, o Santander respondeu que seus **aplicativos bancários possuem mecanismos de segurança para identificar o acesso remoto ao celular e a presença de softwares maliciosos, utilizados como proteção contra fraudes e golpes financeiros**. Informou que a segurança dos dados e a proteção dos clientes são prioridades para o banco, que emprega diversas camadas de segurança em seus sistemas, incluindo anti-robôs, identificação de softwares com acessos privilegiados, criptografias, modelos estatísticos em tempo real para detecção de anomalias no comportamento habitual dos clientes e autenticações por senhas e tokens dinâmicos. Essas medidas seriam escalonadas conforme o risco calculado pelas soluções do banco. O Santander também destacou que mantém sigilo absoluto sobre suas camadas de solução, considerando a sensibilidade do tema, a fim de proteger seus clientes.

Apesar disso, o banco Santander **não especificou claramente em sua resposta se seria capaz de bloquear transações feitas via acesso remoto**. Embora tenha mencionado a existência de mecanismos de segurança em seus aplicativos para identificar acesso remoto ao celular e softwares maliciosos, não ficou claro se esses mecanismos têm a capacidade de bloquear efetivamente as transações feitas por acesso remoto.

Por fim, uma vez que o banco Bradesco encontrou dificuldades em compartilhar sua resposta na íntegra frente aos questionamentos da primeira carta, acabou por reunir os esclarecimentos em uma única resposta apresentada em 20 de junho de 2023, conforme destacado acima. Portanto, não houve apresentação de alegações novas após envio da segunda carta.

Enquanto o Itaú afirmou possuir uma medida específica de segurança para impedir tentativas de transações feitas via aplicativos de acesso remoto, os outros bancos, como Nubank, Santander e Bradesco, não forneceram informações detalhadas sobre medidas concretas para prevenir esse tipo de golpe.

Essa discrepância gera questionamentos sobre a eficácia das políticas de segurança adotadas pelos bancos em geral. **Se um banco é capaz de implementar uma medida efetiva para bloquear transações feitas por acesso remoto, é razoável esperar que os demais também possam fazer o mesmo, dada a importância da segurança das transações financeiras para seus clientes.**

Essa análise crítica levanta preocupações sobre a **responsabilidade das instituições financeiras em garantir a proteção dos dados e recursos de seus clientes, especialmente em um contexto cada vez mais digital e suscetível a golpes cibernéticos**.

Visando avaliar na prática os mecanismos de segurança dos aplicativos, a equipe de Serviços Financeiros do Idec, a partir da contribuição de três voluntários correntistas nas instituições financeiras mencionadas, elaborou um teste visando averiguar se os aplicativos bloqueariam tentativas de transações bancárias feitas via ferramentas de acesso remoto.

04
TESTE PRÁTICO DOS APLICATIVOS

Em 24 de julho de 2023, a equipe de Serviços Financeiros do Idec realizou teste operacional nos aplicativos do Nubank, Itaú, Santander e Bradesco. A escolha dos quatro bancos se justifica pelo levantamento inicial das medidas descritas por estas instituições financeiras para evitar que seus clientes fossem vítimas do golpe do celular invadido.

O teste foi realizado por três voluntários, apresentados neste relatório como Consumidor A, Consumidor B e Consumidor C. O Consumidor A testou o Nubank e o Bradesco. Já o Consumidor B testou o banco Santander, Por fim, o Consumidor C testou o Banco Itaú.

Não se busca atingir um nível de rigor científico nos resultados obtidos por meio do teste de segurança em aplicativos. Evita-se a utilização do termo “estudo”, preferindo-se a denominação de teste. Entretanto, os **resultados indicam claramente a presença de falhas nos sistemas de segurança de alguns aplicativos bancários no contexto brasileiro.**

O teste de segurança não tem a intenção de se configurar como uma pesquisa científica estrita. Não se almeja afirmar que os resultados do teste refletem a situação ampla sobre segurança dos aplicativos bancários. O propósito subjacente aos testes de segurança é conduzir uma avaliação que possua objetivos instrutivos e de relevância política. Aqui, também desejamos conscientizar as pessoas consumidoras para que tenham uma melhor percepção sobre a integridade dos dados em uma tecnologia do cotidiano e compreendam as vulnerabilidades dos aplicativos, incitando a formação de uma “consciência jurídica” e uma compreensão mais profunda das questões de segurança cibernética.

4.1. RECURSOS UTILIZADOS

Foram utilizados computadores, smartphones e um software de acesso remoto para a realização do teste.

4.2. PROCEDIMENTOS

O objetivo era saber se os voluntários conseguiriam acessar seus respectivos aplicativos bancários e realizar transações bancárias por PIX, no valor de R$ 2,00. A tentativa de transação ocorreu a partir do controle das funcionalidades do dispositivo móvel por meio do software de acesso remoto utilizado em computadores.

4.3. RESULTADOS

4.3.1. NUBANK

O teste do aplicativo Nubank foi realizado pelo Consumidor A no dia 24 de julho de 2023, por volta das 10h30 da manhã. No teste, que não será descrito aqui por questões de segurança, o aplicativo do Nubank conseguiu ser acessado pelo software de acesso remoto. Ao entrar na conta do voluntário, foram detectados obstáculos que dificultaram a realização da transação. Porém, **mesmo com esses obstáculos, foi possível realizar a transação.**

4.3.2. BRADESCO

Os mesmos procedimentos foram realizados pelo Consumidor A com relação ao aplicativo do Banco Bradesco. O teste ocorreu por volta das 12h da tarde do dia 24 de julho de 2023. No caso do Bradesco, diferentemente do Nubank, **não houve impedimento ou obstáculos para realizar toda a transação via acesso remoto, fato que indica grave vulnerabilidade do banco**.

4.3.3. ITAÚ

O teste do aplicativo do banco Itaú foi realizado pelo Consumidor B, no dia 24 de julho de 2023, por volta das 10h30 da manhã. O aplicativo do Itaú foi o único que **bloqueou de imediato as tentativas por acesso remoto**. Ou seja, não permitiu que o aplicativo do banco fosse acessado pelo software. Além de também mostrar uma mensagem de suspeita de golpe e bloquear o próprio aplicativo do banco até que o software de acesso remoto fosse deletado do smartphone.

Com esse resultado, o teste chegou ao seu objetivo que era o de mostrar que é possível barrar completamente o golpe do celular invadido ao não permitir o acesso ao aplicativo do banco por meio de softwares de acesso remoto. Logo, **esse golpe só ocorre por conta de uma falha de segurança nos aplicativos dos bancos que não bloqueiam o acesso remoto**.

4.3.4. SANTANDER

Por fim, o Consumidor C realizou o teste do aplicativo do banco Santander no dia 24 de julho de 2023, por volta das 10h30 da manhã. O resultado do Santander foi o mesmo do Nubank. É possível acessar remotamente. Ao entrar no aplicativo, ele cria alguns obstáculos, mas, mesmo com eles, é possível completar a transação.

4.4 RESPOSTAS DOS BANCOS AOS TESTES

Como já foi dito, o objetivo desse teste era mostrar se pessoas leigas, sem entendimento de segurança cibernética, conseguiriam ou não acessar os aplicativos dos bancos a partir de um software de acesso remoto. A conclusão dos testes é de que os **bancos conseguem barrar esse golpe** já no início, já que no teste realizado com o Itaú o banco conseguiu fazer isso.

Assim, o Idec afirma a posição de que o golpe do celular invadido pode e deve ser evitado pelos bancos. **Qualquer vítima que tenha sofrido esse golpe em específico, tem direito à restituição dos valores, o cancelamento dos empréstimos feitos em nome dela, além da retirada da negativação, caso tenha ocorrido**.

Já que é possível que o banco barre a entrada do golpista que utiliza softwares de acesso remoto, o golpe só ocorre por conta da falha de segurança que é, exatamente, permitir a entrada do golpista no aplicativo e a realização da transação.

Após a realização dos testes, o Idec entrou em contato com os quatro bancos. O Santander enviou uma resposta por ofício. Os demais bancos solicitaram uma reunião presencial com o Idec que foi atendida pelo Instituto.

A seguir, listamos as respostas de cada um dos bancos e uma tabela que traz os resultados dos testes em relação às respostas finais dos bancos.

	O teste mostrou que consegue bloquear o acesso remoto ao aplicativo do banco	Após o teste, disse que vai bloquear o acesso remoto ao aplicativo do banco	Trouxe obstáculos durante o teste, mas sem bloquear o acesso remoto ao aplicativo do banco	Não bloqueia o acesso remoto, mas diz que barra transações suspeitas
Bradesco				X
Itaú	X			
Nubank		X	X	
Santander			X	

4.4.1 NUBANK

Em reunião, o Nubank afirmou que com os obstáculos criados e observados no teste feito pelo Idec, a probabilidade do golpe do celular invadido ocorrer era mínima. Para o Idec, mesmo com esses obstáculos, existiam riscos para o consumidor e uma falha de segurança do banco.

Porém, a partir de todo o trabalho do Idec, o Nubank informou que agora está implementando novas medidas de segurança que **bloqueiam efetivamente o golpe do celular invadido** a e que já tem um mecanismo complexo de defesa a golpes e fraudes, inclusive com análise do comportamento do consumidor no aplicativo.

4.4.2 BRADESCO

Durante a reunião realizada com o Idec, o Bradesco afirmou que, apesar de **não apresentar obstáculos no acesso remoto ao aplicativo do banco**, faz uma análise de comportamento em cada uma das transações realizadas pelos consumidores. Quando o comportamento é estranho ou feito por robô, o banco diz que entra em contato com o consumidor ou até bloqueia a transação.

Porém, para o Idec, é **essencial que os aplicativos dos bancos bloqueiem efetivamente as tentativas de acesso remoto** para que o golpe seja realmente evitado. Conforme o Código de Defesa do Cconsumidor, o risco da atividade negocial não pode ser repassado

para o consumidor, já que os produtos e serviços colocados no mercado de consumo devem ser seguros.

4.4.3 ITAÚ

O Itaú foi o único banco entre os testados que **apresentou nos testes o bloqueio efetivo ao golpe do celular invadido**. Durante a reunião com o Idec, o banco trouxe outras medidas de segurança que possui, incluindo análises de comportamento do consumidor e tecnologias de inteligência artificial.

4.4.4 SANTANDER

O Santander respondeu que os obstáculos encontrados no teste feito pelo Idec mostram o investimento do banco na área de segurança e que também trabalha em novas formas de garantir a proteção dos consumidores.

Porém, para o Idec, ainda é preciso criar um mecanismo que **bloqueie completamente o golpe do celular invadido**, o que não foi apresentado pelo banco.

Não há consenso entre os bancos sobre bloquear o acesso remoto como medida de segurança. Entre os quatro bancos, dois (Itaú e Nubank) se mostraram favoráveis, apesar de somente o Itaú de fato ter a prática. Enquanto o Nubank, alvo das demandas de consumidores, admite ter desenvolvido a solução de forma parcial para os seus clientes. Por outro lado, nos outros dois bancos (Bradesco e Santander), o uso não é visto como obstáculo e ambos admitem possuir diversas camadas de autenticação para consolidar a operação, portanto não avaliam o acesso remoto como risco direto.

Para o Idec, mesmo com camadas de autenticação, uma vez apresentada uma falha, o consumidor sempre será responsabilizado pela fraude, porque o banco irá alegar que as camadas existentes garantem o bloqueio da fraude. Mas como saber quando é fraude, se são permitidas as operações remotamente? Como saber que as barreiras não apresentam falhas? Por isso, **O IDEC AFIRMA E REAFIRMA A SUA POSIÇÃO DE QUE OS BANCOS TÊM QUE BLOQUEAR QUALQUER TENTATIVA DE USO DE SOFTWARE DE ACESSO REMOTO EM SEUS APLICATIVOS. CASO CONTRÁRIO, COM A OCORRÊNCIA DO GOLPE, É UM SINAL EVIDENTE DE FALHA DE SEGURANÇA.**

05
CONCLUSÕES

O Idec afirma a importância de todo o trabalho feito sobre o golpe do celular invadido. Após o envio das notificações, os testes e as reuniões com os bancos, ficou evidente que **as mudanças e avanços na segurança dos aplicativos têm ligação direta com o trabalho realizado pelo Idec nestes meses**. Os próprios bancos revelaram isso nas reuniões junto ao Instituto.

Diante do presente relatório, foi possível constatar diferenças significativas entre os mecanismos de segurança utilizados pelos bancos Nubank, Itaú, Bradesco e Santander para prevenir e reparar perdas de consumidores vítimas do golpe do celular invadido.

As respostas do Banco Nubank às notificações e o seu desempenho no teste prático mostraram que o **banco buscou aprimorar seus mecanismos de segurança desde o início do tratamento da questão pelo Idec**, em abril de 2023.

Do mesmo modo, conforme sua resposta à segunda notificação do Idec, **o banco implementou um mecanismo que dificulta a operacionalização do golpe do acesso remoto**. Contudo, é válido destacar que, **ainda assim, o aplicativo apresentou vulnerabilidades na medida em que o acesso remoto ainda fica habilitado a manusear e inserir informações. Além disso, a transação bancária pode ser concluída no dispositivo móvel, ainda que tal dispositivo estivesse sendo acessado à distância por um computador**. Com a resposta aos testes, **o Nubank afirmou que está implementando uma medida que bloqueia de fato esse tipo de golpe.**

Já o Banco Itaú demonstrou um **desempenho satisfatório no teste e condizente com a sua resposta à notificação do Idec**. O aplicativo bloqueou o acesso e não permitiu ser operado pelo consumidor enquanto o dispositivo móvel estava sendo acessado remotamente. Além disso, bloqueou temporariamente o acesso às transações e enviou mensagem informando o consumidor sobre movimentações suspeitas. Assim, restou demonstrada a **eficácia de suas medidas de prevenção, devendo elas serem consideradas paradigmáticas para as demais instituições financeiras**.

O Banco Santander, semelhante ao Nubank, apresentou medida de segurança que dificulta a operacionalização do teste. Para o Idec, essa medida é vulnerável**, representa um risco para os clientes e mostra a necessidade de melhorias nas medidas de segurança do banco**. Na resposta ao teste, o Santander não trouxe novidades a respeito do bloqueio efetivo aos softwares de acesso remoto ao aplicativo do banco.

Por fim, o banco Bradesco apresentou o **pior desempenho no teste prático, permitindo o acesso remoto de seu aplicativo e a realização de transações via Pix**. Durante o teste do aplicativo do banco, não se constatou **nenhuma barreira** específica para esta modalidade de golpe. Em resposta ao teste, o Bradesco afirmou que realmente não bloqueia o acesso remoto, mas que impede ou dificulta transações que fogem do padrão e são consideradas suspeitas.

O objetivo do teste era mostrar que **existe no mercado uma tecnologia que barra o golpe do celular invadido**. Com isso, é **obrigação de toda e qualquer instituição financeira ter essa tecnologia**. Tal constatação reforça o fato de **já existirem medidas de segurança eficazes no mercado capazes de impedir o golpe do celular invadido, devendo a ausência de tais medidas ser interpretada como falha de segurança das instituições financeiras**.

Essa é a interpretação consolidada na **Súmula nº 479 do Superior Tribunal de Justiça (STJ)**, que informa que as instituições financeiras respondem objetivamente por danos decorrentes de fortuito interno, sendo a ausência de medida de segurança contra o acesso remoto um exemplo disso. Portanto, conforme entendimento do STJ, **constatada a falha de segurança dos aplicativos bancários, as instituições financeiras respondem às eventuais perdas dos consumidores de forma objetiva, devendo ressarcir seus respectivos clientes vítimas do golpe do acesso remoto**.

Mesmo diante da existência de supostas ferramentas inibitórias de fraudes, a responsabilidade objetiva das instituições bancárias não deve ser afastada, uma vez que o Código de Defesa do Consumidor visa proteger o patrimônio de seu tutelado contra qualquer conduta indevida.

Verifica-se que a ocorrência de fraudes demonstra a vulnerabilidade do consumidor e o ordenamento consumerista busca proteger os mais frágeis na relação de consumo, visando sempre o reequilíbrio entre as partes. É evidente a responsabilidade dos bancos na prevenção a fraudes e golpes dentro de seus serviços e a garantia de que o consumidor

tenha a adequada proteção contra mecanismos de engenharia social que se utilizam de fragilidades do sistema de segurança digital, como determinado pelo sistema de proteção e defesa aos consumidores.

Agrava-se o fato quando o golpe é realizado contra o consumidor idoso, já que a lei o considera um hipervulnerável e, portanto, ele acaba sendo a principal vítima das fraudes bancárias no ambiente digital.

Conforme a pesquisa de inclusão digital dos idosos realizada pelo **Ipespe**, 70% (setenta por cento) dos consumidores idosos não se sentem seguros no meio digital, apontando as fraudes e os golpes como as principais causas de insegurança desta parcela de consumidores ao utilizar os meios digitais.

Diante da lesão ao consumidor, proporcionada pela má prestação de serviço bancário em razão das fraudes, o Código de Defesa do Consumidor garante a **integral indenização como forma de reparação dos danos patrimoniais**, conforme previsto em seu artigo 6º, inciso VI da norma, através do princípio da prevenção e reparação integral de danos.

Este relatório está disponível para consulta e utilização por parte de consumidores vítimas do golpe do celular invadido. Ele **não é uma garantia de restituição do dinheiro perdido ou de vitória em caso de processo judicial**, mas serve como um instrumento para auxiliar o consumidor a ter o seu dinheiro de volta. O Idec está e sempre estará ao lado das pessoas consumidoras!

******