GOLPES CRESCEM, CAUSAM PREJUÍZOS BILIONÁRIOS E SURFAM NA ONDA DAS NOVAS TECNOLOGIAS

Aldemario Araujo Castro
Advogado
Mestre em Direito
Procurador da Fazenda Nacional
Brasília, 9 de junho de 2023

I. Crescem os golpes e os prejuízos

"Epidemia" de perfis fakes e golpes do pix pela internet geram prejuízos para consumidores. Novas modalidades de crimes praticados com uso de tecnologia tem gerado dores de cabeça para clientes e consumidores e prejuízos para donos de bares e restaurantes (fonte: bandab.com.br).

Bandidos copiam voz e rosto de pessoas para aplicar golpes. Vítimas reconhecem as características de um conhecido e acabam realizando transferências (fonte: recordtv.r7.com).

O número de golpes e fraudes associados ao PIX têm crescido no país, apontam especialistas. Esses ataques acontecem tanto por meio de vírus instalados sem que o consumidor perceba, como via engenharia social (quando um criminoso usa influência e persuasão para enganar e manipular pessoas e obter senhas de acesso) (fonte: g1.globo.com).

Os números são alarmantes. Apenas no mês de janeiro [de 2023], os brasileiros sofreram 284 mil tentativas de fraudes, segundo a Serasa Experian. Ou seja, a cada 9 segundos há uma tentativa de golpe. E o setor mais afetado é exatamente o financeiro. Pelas estatísticas da Serasa, fraudes contra bancos, cartões e financeiras representaram 66% do total (fonte: estadao.com.br).

O aumento do número de fraudes não é exclusividade do Brasil. Pesquisa feita pela empresa de consultoria KPMG, divulgada em 2019, com 43 bancos de todas as regiões do mundo, apurou que mais da metade dos entrevistados anotou incremento no valor e no volume das fraudes, incluindo roubo de identidade e de contas, ataques cibernéticos e golpes de pagamentos supostamente autorizados. Para os bancos, a conta é alta. Embora a pesquisa não informe os valores envolvidos nesses golpes, relata que mais da metade dos entrevistados recuperou menos de 25% das perdas (fonte: estado.com.br).

Esses são cinco exemplos de notícias veiculadas nas últimas semanas acerca de golpes realizados por intermédio de ligações telefônicas e vários tipos de mensagens via internet. Três características são marcantes: a) o crescimento acelerado das ocorrências; b) os prejuízos cada vez maiores (para as pessoas físicas de uma forma geral, bancos e empresas) e c) a exploração das possibilidades abertas pelas novas tecnologias, como a inteligência artificial.

Em 2022, no Brasil, os golpes online causaram um prejuízo estimado de 550 milhões de reais. Foram mapeadas, em média, 17 tentativas de fraude envolvendo os dispositivos eletrônicos, como celulares ou computadores, por hora. Essas informações integram um levantamento realizado pela plataforma de compra e venda online OLX e pela AllowMe, ferramenta de prevenção à fraude e proteção de identidades digitais (fonte: uol.com.br). O Brasil ocupa o sexto lugar do ranking dos países que mais sofrem fraudes na internet. Em 2021, calcula-se que mais de 150 milhões de brasileiros foram vítimas de golpes virtuais (fonte: contaazul.com).

Segundo o aludido estudo, a maioria dos brasileiros vítimas de fraudes é jovem, com idade até 31 anos. Os homens representam 74% e as mulheres 26%. O senso comum indica que as pessoas mais idosas, com maiores dificuldades de lidar com as novas tecnologias, seriam as vítimas mais frequentes. Ocorre que o público mais jovem tem uma presença mais ativa no mundo digital, utiliza as transações online com mais intensidade e, portanto, fica mais exposto aos riscos.

Outra conclusão interessante aponta que 70% das tentativas de fraude aconteceram em horário comercial. A quinta-feira foi o dia da semana com maior número de ocorrências.

A crescente visibilidade e utilização da inteligência artificial em 2023 também atraiu a atenção das mentes criminosas voltadas para os golpes ou fraudes online e congêneres. Já são encontrados relatos apontando o uso da inteligência artificial para imitar a voz de pessoas e enganar amigos e parentes em busca de dinheiro fácil.

Em regra, o criminoso realiza uma ligação telefônica para uma pessoa e desenvolve uma conversa com duração razoável. Assim, faz-se a captação da voz. Na sequência, um parente ou amigo próximo recebe uma ligação que reproduz, mediante recursos de inteligência artificial, a voz da pessoa que foi o primeiro alvo da operação. A voz familiar enfraquece ou anula as cautelas e desconfianças. Assim, transferências bancárias e operações afins são efetivadas, especialmente porque se cria um contexto de urgência para a realização das transações.

A clonagem (ou simulação) de voz via inteligência artificial foi utilizada recentemente num golpe de falso sequestro no Arizona, EUA. Jennifer DeStefano, mãe de uma adolescente de 15 anos, atendeu uma ligação telefônica e ouviu a filha em prantos. “Era a voz dela. Era a entonação dela. Era assim que ela teria chorado. Nunca duvidei nem por um segundo que fosse ela. Essa é a parte esquisita que realmente me deixou preocupada”, disse Jennifer para a imprensa americana (fonte: olhardigital.com.br).

Recentemente, “um influencer de São Paulo denunciou nas redes sociais que teve a voz clonada por meio de inteligência artificial (IA) e que o recurso foi utilizado para aplicar um golpe no pai dele. O homem perdeu R$ 600 ao receber uma ligação, supostamente do filho, pedindo um empréstimo” (fonte: g1.globo.com). Na postagem, o aludido influenciador digital apontou um forma simples de evitar golpes envolvendo os membros de uma família. A providência consistente na criação de uma palavra de segurança (senha) compartilhada entre os familiares e solicitada para confirmar a identidade de quem faz algum tipo de contato envolvendo questões financeiras ou similares.

II. Os golpes mais comuns

Segundo os especialistas em segurança digital, esses são os golpes mais comuns na atualidade:

1. Golpes de clonagem e novo número no WhatsApp. Existem várias maneiras de realizar a clonagem, inclusive aquelas em que se obtém acesso ao código de seis dígitos enviado por mensagem de texto à vítima. Para obter esse número, o golpista aparenta ser um atendente de suporte técnico ou de um setor de cobrança. Também são enviadas mensagens contendo links maliciosos que levam a vítima para páginas falsas que solicitam informações pessoais por meio do preenchimento de formulários. Esses links podem direcionar o usuário para páginas com vírus usados para clonar a conta da pessoa. O golpe do novo número é realizado pelo criminoso que já possui acesso aos números da agenda telefônica da vítima. O golpista cria uma nova conta no WhatsApp e utiliza uma foto capturada em redes sociais para enviar mensagens aos contatos. Solicita-se dinheiro para resolver alguma situação delicada ou urgente sob a alegação de que houve mudança no número de telefone anteriormente usado.

2. Golpe do suporte técnico falso. Neste caso, o criminoso se passa por funcionário de grandes empresas via WhatsApp, ligação telefônica ou mensagem de correio eletrônico. Normalmente, solicita-se a realização de uma ação ou procedimento com urgência.

3. Golpe do marketing multinível (ou pirâmide financeira). A vítima é contatada nas redes sociais ou via WhatsApp. Faz-se, então, uma proposta tentadora. A pessoa receberá o dobro ou mais do valor que depositar. Em regra, a vítima recebe alguns valores menores e é estimulada a realizar novos depósitos e convidar amigos e parentes. Depois de algum tempo e de transferências cada vez maiores, os golpistas literalmente desaparecem.

4. Golpe da vaga de emprego. Com milhares de casos registrados, os criminosos utilizam os nomes de grandes empresas para obter dados e dinheiro das vítimas interessadas em conseguir um posto de trabalho. Os golpistas informam que a participação num processo seletivo ou a própria contratação exige o pagamento de algum tipo de taxa. A possibilidade iminente de conseguir um emprego leva a vítima a fornecer informações pessoais e transferir recursos pecuniários. Na sequência, resta a frustração.

5. Golpe do falso boleto. A vítima recebe um boleto falso por mensagem de correio eletrônico ou carta física. Indica-se que se trata de uma cobrança urgente ou algo parecido com uma série de consequências negativas caso não ocorra o pagamento. O documento parece verídico, mas não passa por uma análise mais cuidadosa de uma série de detalhes.

6. Golpe do falso pagamento. Conta com a falta de cuidado da empresa ou pessoa física que não confirma os valores recebidos em conta bancária. Nesses casos, o comprovante enviado pode ter sido adulterado ou o pagamento agendado é cancelado posteriormente.

7. Golpe do falso empréstimo. Os fraudadores criam sites e inserem anúncios em páginas de pesquisas, usando, inclusive, nomes de bancos famosos. Os sites parecem verdadeiros, no nome, no endereço eletrônico e no layout. A vítima, devidamente enganada pelos golpistas, fornece todos os dados pessoais. Segue-se um contato com o anúncio da existência de empréstimo pré-aprovado. Solicita-se a realização de depósito inicial de abertura de conta ou algum tipo de taxa para liberação do valor do empréstimo. Depois, como em outros golpes, “tudo” desaparece.

8. Golpe da falsa central de atendimento. O fraudador faz contato telefônico com a vítima como se a ligação partisse do banco dessa última. Registre-se a existência de softwares que permitem mostrar para a vítima exatamente o número do banco ou qualquer outro. Então, o golpista avisa sobre uma suposta operação irregular, pede a confirmação de vários dados pessoais e direciona a vítima para o setor de segurança do banco. Nesse segundo momento, são solicitadas senhas ou orientada a

instalação de softwares que realizarão o monitoramento do uso de celulares ou computadores de mesa.

9. Golpe do falso motoboy. Assim como no golpe da falsa central de atendimento, o meliante se apresenta como funcionário do banco da vítima. Informa, logo depois, que um ou vários cartões de crédito foram clonados e um motoboy recolherá o(s) plástico(s) correspondente(s). As senhas e outros dados sensíveis também são solicitados e utilizados em compras e operações bancárias.

10. Golpe da venda de produto usado. O criminoso invade a conta de uma vítima em uma rede social, como o Instagram, e faz publicações oferecendo produtos com preços acessíveis e atraentes. Para tornar a fraude mais convincente, os golpistas estudam as características de como o proprietário da conta escreve e tentam imitá-lo o máximo possível. Geralmente, esses criminosos anunciam que estão se mudando e precisam vender seus pertences. Depois disso, o golpista solicita um pagamento adiantado por meio de um pix ou transferência bancária. Depois de enviado o valor, o contato com a vítima é encerrado.

11. Golpe do pix. Os fraudadores enviam mensagens de texto oferecendo descontos em faturas de celular ou cartão de crédito se o pagamento for feito através de pix. Para tornar o processo mais rápido e fácil, eles incluem um QR Code para o pagamento diretamente na mensagem de texto. Outro esquema de fraude com pix envolve uma suposta parceria entre empresas de cartões de crédito que oferece descontos de até 40% nas faturas. A vítima é redirecionada para um site falso e é solicitado que informe seu CPF, o valor da fatura a ser paga, a bandeira do cartão e os últimos quatro dígitos do número do cartão de crédito para gerar o QR Code com o suposto desconto.

12. Golpe da troca de cartão. Ocorre quando a vítima está pagando suas compras em lojas ou outra situação em que utiliza o cartão de crédito. O golpista presta atenção na digitação da senha na máquina e, nos segundos seguintes, enquanto aguarda a aprovação da transação, realiza uma rápida troca do cartão por um falso.

13. Golpe do cartão extraviado. Os fraudadores conseguem um cartão físico em nome da vítima que será alvo do golpe. Inúmeras vezes o cartão pode ser interceptado em algum momento do fluxo postal. Depois de obter o cartão, os bandidos entram em contato com a vítima e pedem sua senha. Alega-se que esse procedimento tornará o processo de solicitação e envio de um novo cartão mais rápido.

14. Golpe das falsas lojas online. São lojas supostamente verdadeiras abrigadas em perfis em redes sociais, como o Instagram e o TikTok, e mesmo em sites. São veiculados produtos com preços baixos e promoções imperdíveis. Podem ser encontradas até avaliações falsas acerca do vendedor e dos produtos. A vítima, ao realizar a compra diretamente pela loja, fornece informações pessoais e faz um pagamento via pix, transferência bancária ou cartão de crédito. Depois de receber o pagamento, a loja bloqueia o usuário. A mercadoria “comprada” jamais é recebida.

15. Golpe das falsas promoções. Perfis e sites falsos de grandes empresas fazem contato por meio de mensagens no WhatsApp ou Instagram e até correio eletrônico. Informa-se que a vítima ganhou uma promoção ou um vale-compra com um valor significativo. Ao clicar no link fornecido, a vítima é direcionada para um site onde será necessário fornecer seus dados pessoais e, em alguns casos, até informações da sua conta corrente para receber o prêmio. Depois de revelar as informações pessoais, a vítima não terá mais acesso ao perfil ou site da empresa.

16. Golpe da videochamada. Certos golpistas criam sites e links que levam a vítima, ao acionar o recurso da videochamada no WhatsApp, a inserir seu número e informar o código de verificação. Capturados esses dados, abrem-se as portas para uma série de fraudes.

17. Golpe do QR Code. O criminoso cria um QR Code falso semelhante ao código legítimo utilizado em alguma operação frequente no mercado de venda de bens e serviços. A digitalização de QR Codes maliciosos: a) direciona o usuário a sites fraudulentos, construídos para obter contas bancárias, cartões de crédito, senhas ou outras informações pessoais sensíveis ou b) viabiliza a instalação de malwares que monitoram todas as ações realizadas num celular. É preciso um especial cuidado com QR Codes de restaurantes e bares. Sobre a imagem legítima

disponibilizada pelo estabelecimento pode ter sido colado um adesivo com um QR Code falso. Assim, o que seria um simples acesso ao cardápio do estabelecimento comercial pode se transformar em um grande transtorno.

III. Os principais cuidados

Os principais cuidados a serem observados para evitar os golpes mencionados, e outros assemelhados, são os seguintes: a) desconfiar de ofertas ou promoções muito vantajosas (com preços muito inferiores ao do mercado); b) não acionar links suspeitos ou abrir anexos de e-mails desconhecidos; c) certificar-se da legitimidade do site antes de inserir informações pessoais ou financeiras. Para tanto: c.1) preste atenção no endereço eletrônico; c.2) verifique os certificados de segurança; c.3) confira em nome de quem o site está registrado no seguinte endereço eletrônico: <registro.br/tecnologia/ferramentas/whois> e c.4) confira o registro do CNPJ no seguinte endereço eletrônico: <www.gov.br/pt-br/servicos/consultar-cadastro-nacional-de-pessoas-juridicas>; d) usar senhas fortes e diferentes para cada fornecedor ou site; e) ativar a autenticação de dois fatores, se possível; f) não compartilhar informações pessoais, como senhas e dados bancários, com desconhecidos ou em sites não confiáveis; g) manter o software antivírus atualizado; h) fazer backups regulares dos dados e arquivos mais importantes; i) atentar para erros de ortografia e gramática em e-mails e mensagens; j) não confiar em ligações ou mensagens que solicitam informações ou possuem alguma implicação financeira, mesmo que pareçam legítimas; k) entrar em contato diretamente com a instituição ou empresa em caso de dúvida ou suspeita e l) manter-se atualizado sobre os tipos de golpes e fraudes mais comuns.

Sugere-se a leitura da “Cartilha de Segurança para Internet”, material produzido pelo CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (cartilha.cert.br/fasciculos). Organizada em fascículos, contempla temas específicos como: a) banco via internet; b) boatos; c) comércio eletrônico; d) furto de celular; e) privacidade; f) proteção de dados e g) redes sociais.

Deve ser dispensada uma especial atenção para a utilização dos celulares. Praticamente todas as comunicações e a vida financeira da maioria das pessoas ocorrem por intermédio de smartfones. Conforme dados do Observatório de Segurança Pública da Secretaria de Estado de Justiça e Segurança Pública de Minas Gerais, a cada 10 minutos um celular foi furtado em Minas nos dois primeiros meses de 2023 (fonte: em.com.br).

No caso de roubo ou furto de celular, as providências recomendadas pelas autoridades policiais e especialistas são as seguintes: a) comunicar imediatamente ao(s) banco(s) e à operadora de telefonia para as providências de bloqueio das contas; b) registrar um boletim de ocorrência presencial ou virtual; c) modificar as senhas dos aplicativos instalados no celular e d) apagar, remotamente, os dados por intermédio dos sites dos fabricantes dos equipamentos.

Entre as medidas de segurança especificamente para celulares são destacadas: a) não manter dados e informações sensíveis armazenados no equipamento; b) não instalar aplicativos fora das lojas oficiais; c) usar o bloqueio automático da tela inicial; d) utilizar as ferramentas de segurança do aparelho; e) evitar deixar o número do cartão de crédito armazenado em aplicativos de compras; f) usar cartões de créditos virtuais e g) bloquear a utilização do SIM Card (o popular “chip”) com senha.

IV. Tratamento jurídico

Em regra, a jurisprudência tem reconhecido que as instituições financeiras possuem responsabilidade objetiva pelos danos causados a seus clientes em decorrência de golpes virtuais, especialmente quando esses são praticados por meio de técnicas de engenharia social voltadas para a obtenção de informações confidenciais dos usuários. As decisões referidas buscam fundamentos no Código de Defesa do Consumidor (art. 14) e nas Súmulas ns. 297 e 479 do Superior Tribunal de Justiça.

Inúmeras decisões judiciais destacam falhas na prestação de serviços bancários relacionados com os golpes antes referidos. Questiona-se a ausência

de providências para evitar ou minimizar as ocorrências de operações em curto espaço de tempo, com valores muito elevados e destoando completamente do perfil de transações do usuário. Assim, não seria viável considerar uma culpa exclusiva do cliente que afastasse a responsabilidade das instituições bancárias.

V. Conclusão

Infelizmente, vivemos num mundo em que o atual estágio de evolução dos indivíduos e da sociedade aponta para a prevalência das ações e comportamentos negativos ou destrutivos. Assim, as cautelas e cuidados precisam ser proporcionais ao potencial de danos e prejuízos emergentes do convívio social com essas características.