

FRAUDES FINANCEIRAS NO BRASIL

JUNHO • 2021



Sistema CNDL



► Fraudes financeiras cresceram 28% na comparação com 2019



O combate à pandemia de Coronavírus impôs a necessidade de distanciamento social e reforçou uma tendência observada há alguns anos: a digitalização dos serviços financeiros. Dados da Federação Brasileira dos Bancos (FEBRABAN)¹ mostram que, mesmo antes do chamado “novo normal”, a participação do Mobile Banking e do Internet Banking no total de transações bancárias vinha crescendo -- o percentual passou de 52%, em 2015, para 63% em 2019.

É razoável supor que, sem o desenvolvimento tecnológico experimentado nos últimos anos, o impacto econômico

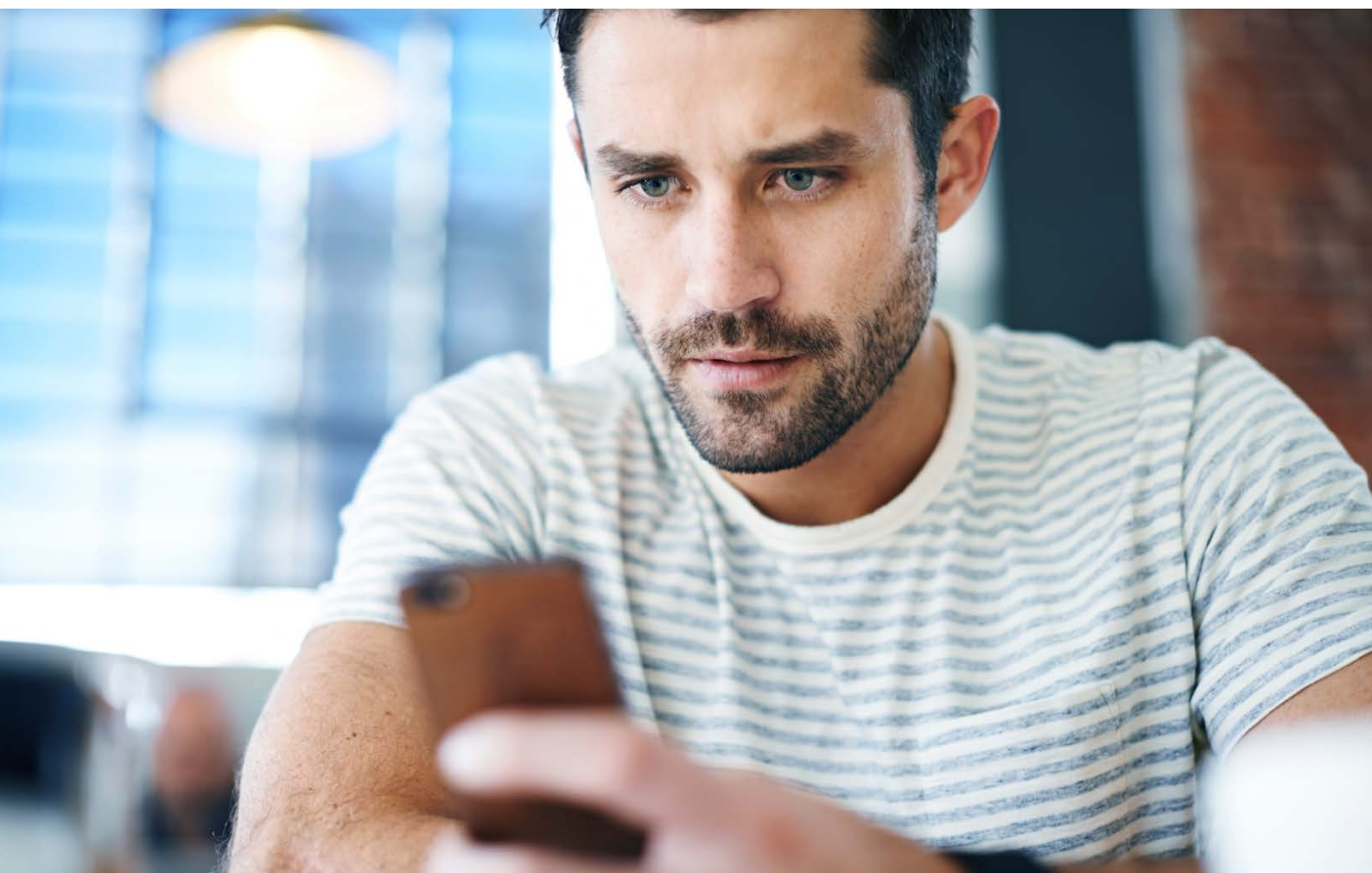
da pandemia teria sido maior. Os meios digitais foram um canal importante para a comercialização de bens e serviços e para distribuição de benefícios públicos, como o Auxílio Emergencial. Mas o mesmo progresso que facilita o cotidiano, reduz as filas, a papelada e gera inúmeras oportunidades também serve para a sofisticação da atuação criminosa. A inovação e a criatividade, em outras palavras, avançam nas duas pontas: tanto para o bem quanto para o mal. Num país ainda carente de educação financeira, e de educação em sentido mais amplo, a ação dos fraudadores torna-se ainda mais facilitada

¹ <https://portal.febraban.org.br/pagina/3106/48/pt-br/pesquis>

Tendo em vista a urgência e a importância do tema, a Confederação Nacional de Dirigentes Lojistas (CNDL), o Serviço de Proteção ao Crédito (SPC Brasil) e o Sebrae realizaram uma nova edição do estudo “Fraudes Financeiras no Brasil”. A pesquisa foi feita pela web e ouviu residentes de todas as capitais brasileiras, com idade igual ou maior que 18 anos, das classes A, B e C, e que foram vítimas de algum tipo de fraude financeira nos últimos 12 meses, seja em instituições financeiras, investimentos, e-commerce e

comércio em geral, entre outras listadas no estudo.

Além de permitir a comparação do quadro atual com aquele traçado em 2019, o estudo traz novas evidências sobre o assunto. Consta-se, por exemplo, que o número de vítimas desses golpes nos últimos 12 meses cresceu, chegando a atingir 16,7 milhões de internautas brasileiros. A pesquisa mostra, ainda, um crescimento das abordagens de ligações e mensagens.

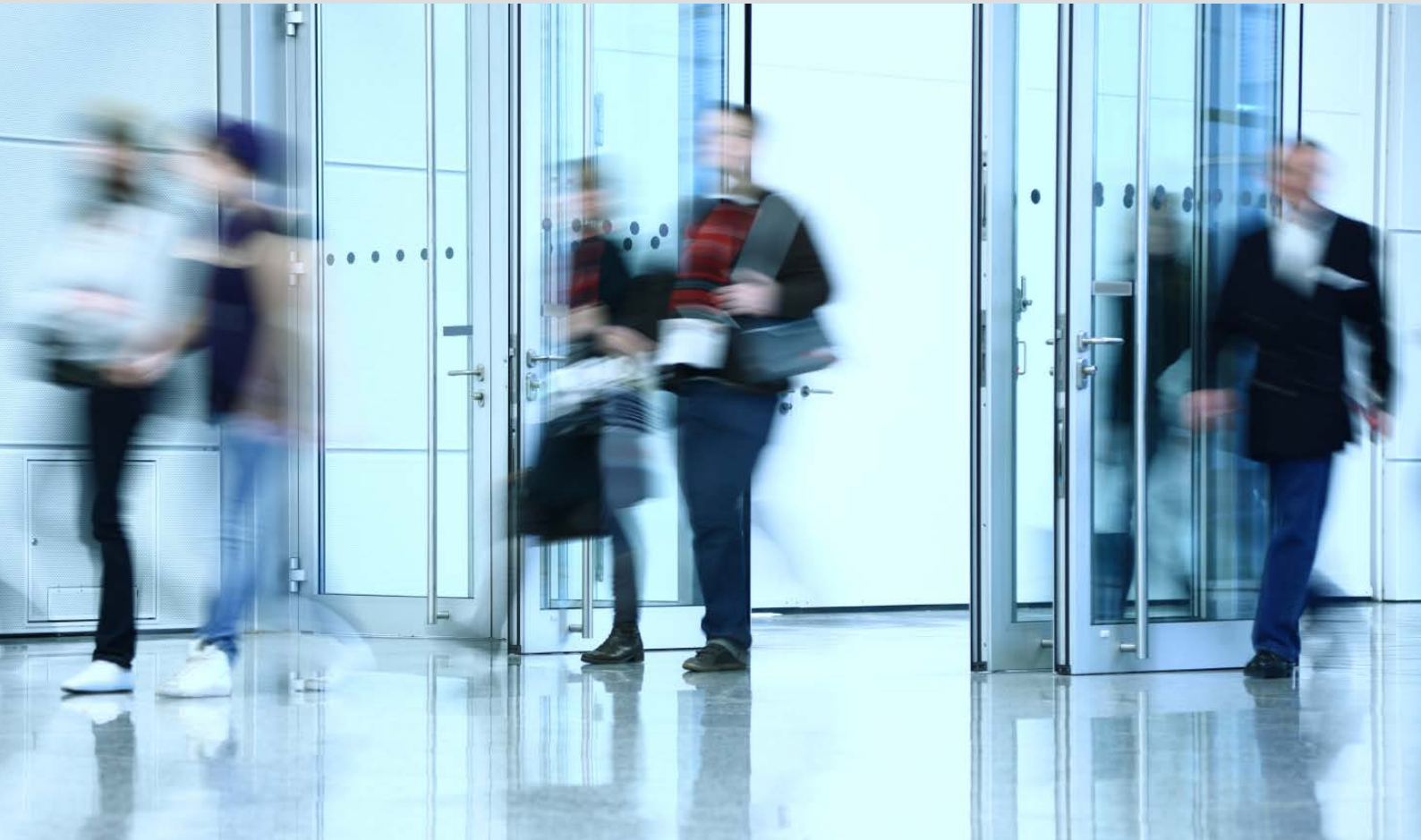


O contexto e os desdobramentos da ocorrência de fraude também foram objetos de investigação do estudo, além do prejuízo acarretado aos consumidores e dos custos para revertê-lo, como gastos com deslocamento, chamadas telefônicas e taxas. O estudo mostra que a perda de documentos e o fornecimento inadvertido de dados, sobretudo através de atualizações cadastrais, e-mail, mensagens instantâneas ou chamadas telefônicas,

são alguns dos fatores que antecederam o golpe e podem ter sido a porta de entrada dos criminosos. Entendendo que o processo de digitalização dos serviços financeiros é irreversível, e que traz consigo um grande potencial econômico, o propósito do estudo é ensinar a conscientização dos consumidores e empresários, e mobilizar o debate público sobre o assunto.

PERFIL DAS VÍTIMAS DE FRAUDE

► Idade média dos internautas que sofreram fraude nos últimos 12 meses é de 39 anos; mais da metade tem ensino médio completo



O perfil dos consumidores que foram vítimas de alguma fraude ao longo dos últimos 12 meses mostra que, no quesito de gênero, não há um alvo preferencial: 50,8% das vítimas são do sexo feminino e 49,2% são do sexo masculino. A idade média dos consumidores fraudados é de 39 anos, sendo que pouco mais da metade (51,5%) têm idade entre 25 e 44 anos, e 16,6% têm idade superior a 55 anos.

Os dados de renda mostram que 26,6% dos consumidores que sofreram algum tipo de golpe financeiro nos últimos 12 meses têm renda familiar entre 1 e 2 salários-mínimos e 19,1% têm renda familiar de 2 a 3 salários-mínimos. Distribuídos por classes sociais, 43,6% pertencem às classes A e B e 56,4% pertencem à classe C. A pesquisa

também constata que, entre esses consumidores, o número médio de residentes por domicílio é de 3,1.

Com relação ao nível de escolaridade, mais da metade dos consumidores entrevistados (53,6%) têm ensino médio completo e cerca de um quarto (25,8%) completaram o ensino superior. Além desses, 7,6% cursaram até o ensino fundamental (I ou II) e 13% cursaram pós-graduação, mestrado, doutorado ou mais.

Por fim, o quadro regional mostra que 51,8% dos consumidores que sofreram fraude estão na região Sudeste; 24,6% estão na região Nordeste; 10,5% na região Centro-Oeste. Sul e Norte concentram, respectivamente, 7,4% e 5,7% desses consumidores.

FRAUDES FINANCEIRAS

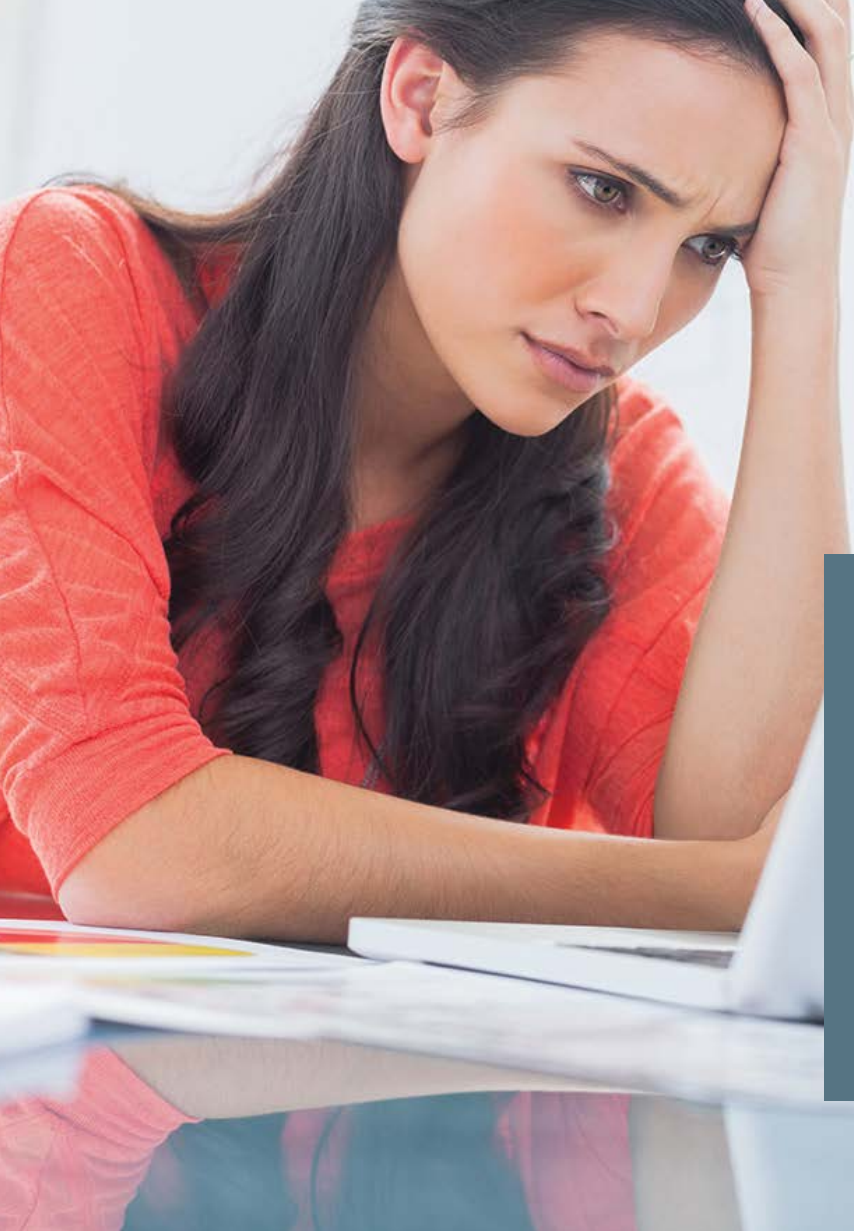
► 16,7 milhões de internautas foram vítimas de algum tipo de fraude financeira nos últimos 12 meses



De tempos em tempos, a sociedade é surpreendida com alertas sobre novos tipos de fraudes. Esse não é um mal apenas dos nossos dias. Um Decreto Lei de 1940² já estabelecia pena de reclusão a quem obtivesse vantagem ilícita, induzindo um terceiro ao erro. Se é verdade que as fraudes são uma prática antiga, também é verdade que o avanço tecnológico e a crescente conectividade do mundo abriram novas possibilidades para os fraudadores.

O problema não reconhece fronteiras. Estudo da empresa McAfee e do “Center of Strategic and International Studies” (CSIS)³ estimou em 0,8% do PIB mundial o custo dos crimes cibernéticos. Esse custo, de acordo com o relatório, vem sendo impulsionado pela adoção de novas tecnologias e, sobretudo, pela maior facilidade de monetização da atividade criminosa.

2 <https://www2.camara.leg.br/legin/fed/decllei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html>
3 <https://www.mcafee.com/enterprise/pt-br/assets/executive-summaries/es-economic-impact-cybercrime.pdf>



Não recebimento de produtos comprados foi a fraude mais apontada, seguida do recebimento de produtos/serviços diferentes do anunciado e da clonagem de cartões

A pesquisa “Fraudes Financeiras no Brasil” constatou que, nos últimos 12 meses, 59% dos internautas brasileiros sofreram algum tipo de fraude financeira, ante 46% em 2019 – um crescimento, portanto, de 28,3% da taxa de incidência. Em termos absolutos, o número de internautas fraudados representa um contingente 16,7 milhões de pessoas. O não recebimento de produtos/serviços comprados liderou a lista de fraudes sofridas, sendo mencionado por 40,9% dos entrevistados. Em termos percentuais, esse número caiu na comparação com 2019 (52,0%), o que mostra uma perda de importância relativa, frente a outros tipos de ocorrência. Observa-se, no entanto, um crescimento do número absoluto de internautas vitimados por essa fraude, que passou de 6,3 milhões, em 2019, para 6,8 milhões em 2020. O e-commerce brasileiro vem crescendo ano após ano,

tendo sido decisivo para sobrevivência de muitas atividades comerciais durante a pandemia. Uma pesquisa da Confederação Nacional de Dirigentes Lojistas (CNDL)⁴ e do Serviço de Proteção ao Crédito (SPC Brasil) sobre compras pela internet, em sites e aplicativos, considerando também as novas formas de aquisição pelas redes sociais e WhatsApp, mostrou que 91% dos internautas utilizaram esse canal nos últimos 12 meses, o que representa quase a totalidade desse universo e um aumento de 5 p.p. na comparação com os dados de 2019. O crescimento do número de compradores online, associado a um menor percentual de incidência de fraudes, observado na presente pesquisa, sugere que a maior experiência dos consumidores com esse meio tende a reduzir esse tipo de ocorrência.

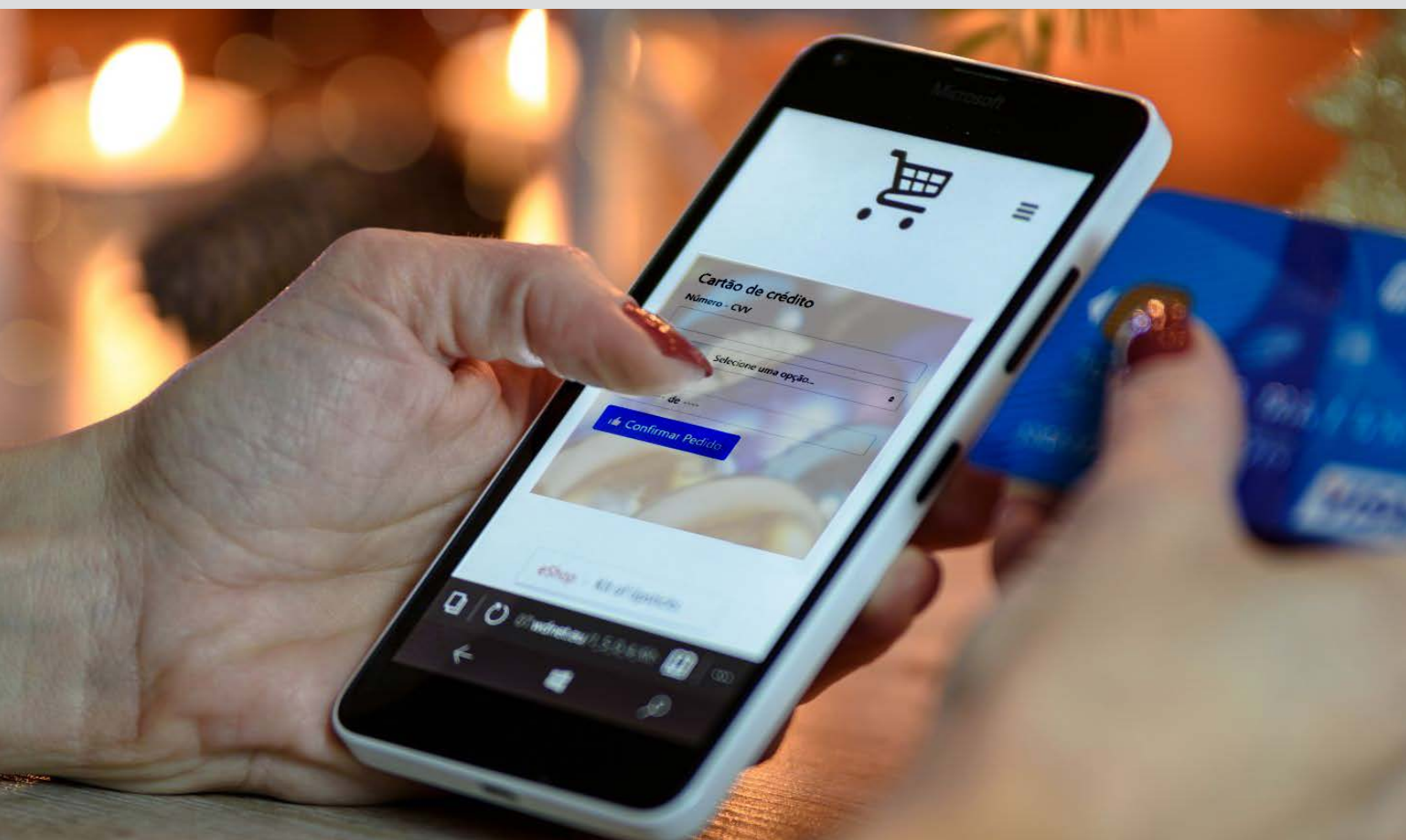
⁴ Disponível em: <https://www.ebit.com.br/webshoppers>



Tipos de fraudes financeiras mais recorrentes

	2019	2021
Não recebi um produto/bem que comprei	52%	41%
Comprei um produto/serviço que veio diferente das informações especificadas pelo vendedor	42%	41%
Tive o meu cartão de crédito/débito clonado	25%	24%
Me envolvi num golpe através de ligação, e-mail, SMS ou WhatsApp de golpistas, informando que eu tinha direito a receber um dinheiro, e para conseguir a quantia, forneci dados pessoais e bancários, além do pagamento de honorários	8%	17%
Realizei o pagamento de falsa cobrança por meio de depósito, boleto falsificado ou adulterado	11%	15%
Perdi dinheiro em investimentos financeiros fraudulentos como: golpe das ações ou fundo de aposentadoria, esquemas de pirâmide financeira	11%	14%
Contrataram serviços ou compraram itens em meu nome usando documentos falsos, perdidos ou roubados (como linha de celular, internet, tv por assinatura, carro, etc.)	14%	13%
Paguei por um serviço que não foi realizado – ex: limpeza de nome, regularização de CNH cassada, empresas que renegociam dívidas, falsas agências de emprego, agências de viagens, produção de festas, entre outros	11%	12%
Fizeram uma transação financeira (saques, pagamentos ou transferências) na minha conta bancária sem minha autorização	13%	11%
Meu número de celular/ WhatsApp foi clonado e utilizado indevidamente para roubo de dinheiro de parentes, amigos	8%	11%
Emitiram cartões de crédito no meu nome sem minha autorização usando documentos falsos, perdidos ou roubados	10%	9%
Vendi um produto pela internet e o comprador recebeu mas não me pagou	10%	7%
Tomaram um crédito em meu nome – empréstimos, financiamento ou crediário – sem minha autorização usando documentos falsos, perdidos ou roubados	7%	7%
Contratei empréstimo falso (a taxas e condições atraentes) com exigência de pagamento antecipado de taxas ou comissões para aquisição	6%	6%
Falsificaram minha assinatura em algum documento ou cheque	7%	5%
Comprei um falso consórcio sorteado/contemplado	4%	4%
Utilizaram minhas milhas ou outros pontos acumulados em programas de fidelidade sem minha autorização* (* Atributo inserido em 2021)	-	4%
Fui abordado em um caixa eletrônico por uma pessoa que fingiu ser funcionário do banco e tive dinheiro desviado da minha conta ou dados roubados	4%	4%
Abriam conta bancária em meu nome sem minha autorização usando documentos falsos, perdidos ou roubados	5%	4%
Clonaram a placa, documentação ou chassi do meu veículo	4%	3%
Abriam empresas em meu nome sem minha autorização	4%	2%

► Eletrônicos e vestuário lideram a lista de itens não recebidos



Os entrevistados que compraram algum item e não receberam detalharam o contexto do não recebimento do produto. De acordo com a pesquisa, 38,7% mencionaram ter feito o pagamento por cartão de crédito e 28,1% apontaram que a empresa era de fachada em site ou perfil de rede social falso, criada apenas com o intuito de aplicar o golpe. Um quinto dos que tiveram esse problema (20,9%) ainda mencionaram o extravio do produto, sem que a empresa responsável fizesse a reposição. Compras feitas diretamente de pessoas físicas, com pagamento através de transferência ou depósito, também foram citadas (16,2%). Entre outras menções, 8,0% apontaram que a empresa encerrou as atividades e não avisou.

Os locais onde as compras não recebidas ocorreram variam, mas, como é fácil supor, há forte prevalência do meio online: 40,5% mencionaram sites que vendem produtos diversos (os chamados marketplaces). Cumpre destacar que esse percentual recuou 26 p.p. na comparação

com 2019 (66,6%). Já os sites de loja específicas foram citados por 28,4%, seguidos de perfis de empresa em rede social (22,7%). A compra de pessoas físicas, seja em rede social (13,4%), seja em sites de produtos novos ou usados (10,3%), também foi lembrada. Nas lojas físicas, mencionadas por 3,4%, o problema mostrou-se bem menos frequente.

Na listagem dos produtos não recebidos, os eletrônicos mantiveram o destaque já observado em 2019. Esses produtos foram citados por 30,4%, com destaque para o público masculino (42,4%). Roupas, sapatos e acessórios (25,3%), e cosméticos e perfumaria (13,7%) apareceram em seguida, mas com destaque para o público feminino. Também tiveram destaque os eletrodomésticos (11,9%) e os remédios e produtos de cuidado para a saúde (5,4%). O valor perdido com os produtos não recebidos chegou a R\$ 140, em média, sendo que para 46,1% ficou abaixo de R\$ 100; 6,2% citaram produtos acima de R\$ 800.

► **Recebimento de produto ou serviço diferente do que foi comprado, clonagem de cartão e golpes através de ligações ou mensagens estão entre as principais fraudes**



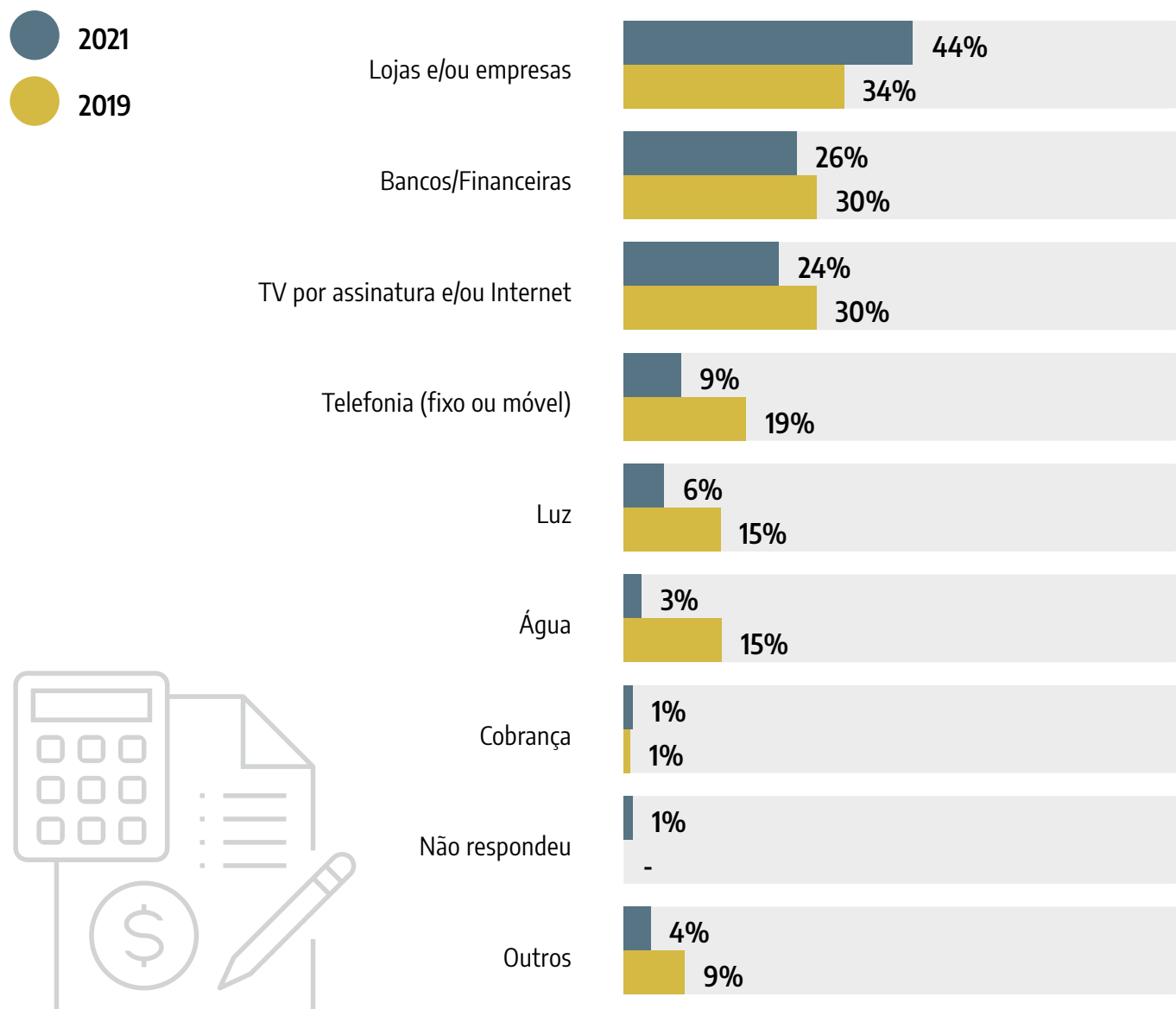
Além da não entrega, 40,6% dos entrevistados mencionaram o recebimento de um produto ou serviço diferente do especificado pelo vendedor. Esse foi o segundo tipo de fraude mais citado na pesquisa.

A clonagem de cartão de débito e crédito foi mencionada por 24,0% dos consumidores que sofreram algum tipo de fraude nos últimos 12 meses. Em seguida, com crescimento expressivo, aparecem os golpes através de ligação, e-mail, SMS ou WhatsApp solicitando dados pessoais e bancários ou pagamento de honorários para o recebimento de dinheiro. Essa fraude foi mencionada por

17,1% dos internautas vitimados de alguma forma, ante 8,4% em 2019.

O pagamento de falsas cobranças cresceu 4 p.p. na comparação com o levantamento anterior, passando de 11%, em 2019, para 15,5%. Entre os internautas que caíram nesse tipo de golpe, as cobranças mais citadas vieram, supostamente, de lojas e empresas (44,2%); de bancos e financeiras (26,5%); de serviços de TV por assinatura e/ou internet (23,8%); e de telefonia fixa ou móvel (8,8%). Até mesmo contas básicas foram citadas, como as de luz (6,1%) e água (2,7%).

Tipos de falsa cobrança que foram pagas por meio de depósito, boleto falsificado ou adulterado

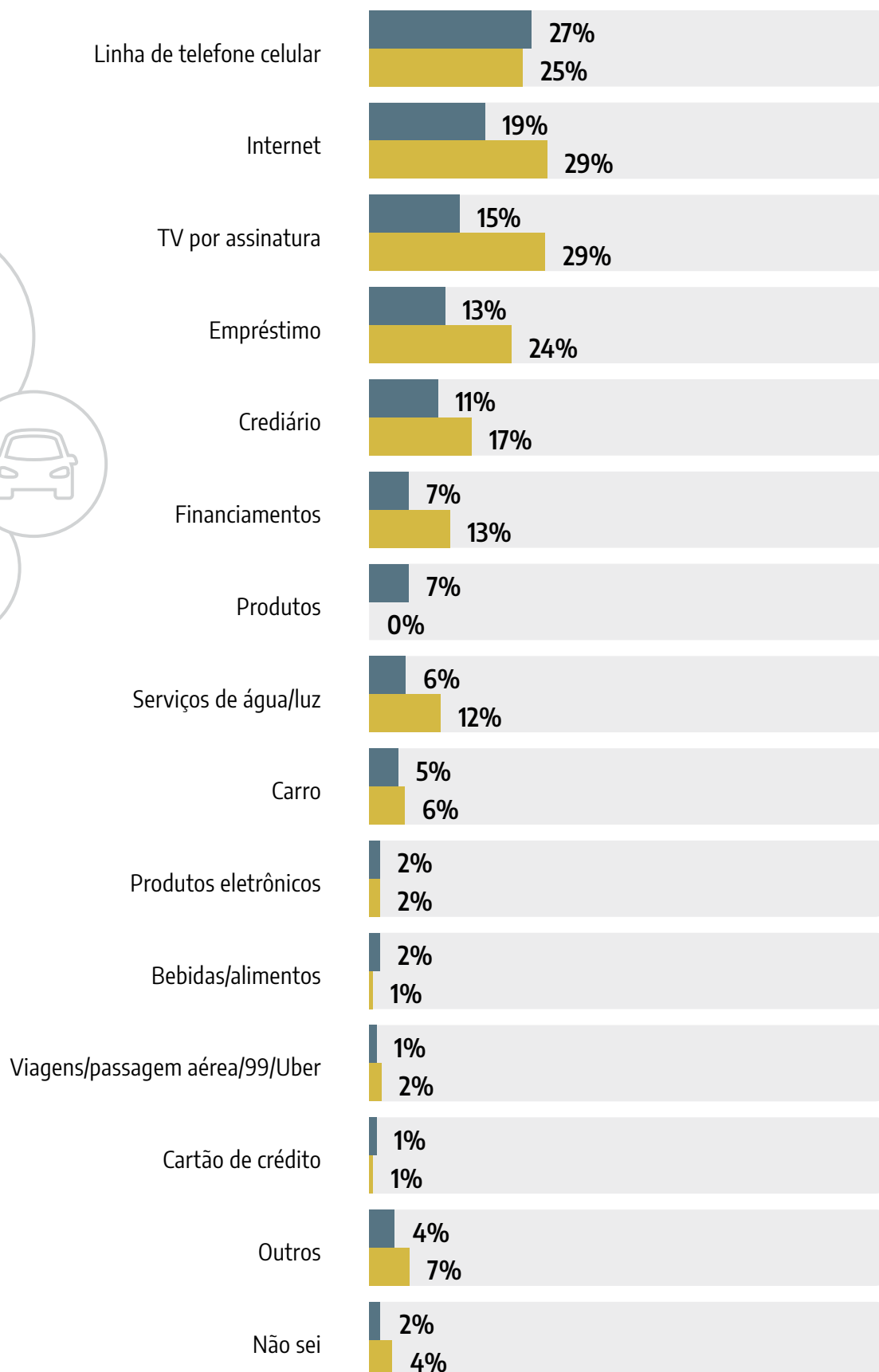
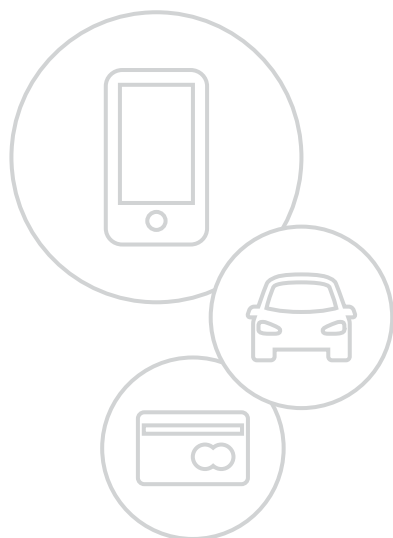


Em tempos de interesse crescente pelo tema dos investimentos e de surgimento de novos ativos, como as criptomoedas, 13,9% foram vitimados com a perda de dinheiro em investimentos fraudulentos, como golpe das ações ou fundo de aposentadoria e esquemas de pirâmide financeira.

De acordo com a pesquisa, 13,2% relataram que o seu nome foi usado para a compra de itens ou contratação de serviços por terceiros, a partir de documentos falsos, perdidos ou roubados. Para aqueles que foram surpreendidos com

a contratação de produtos em seu nome, as linhas de telefone celular foram o tipo de contratação mais citada, lembradas por 26,9% dos entrevistados. A contratação de internet registrou queda de 10 p.p. no número de citações na comparação com 2019 (19,2%, ante 29,5% observado no estudo anterior). O serviço de TV por assinatura foi mencionado por 15,0% em 2021, ante 29,2% em 2019. Também houve contratação de crédito no nome dos entrevistados: empréstimos, crediário e financiamentos foram citados por, respectivamente, 12,6%, 11,4% e 6,6% dos que sofreram esse tipo de fraude.

O que foi contratado ou comprado em seu nome usando documentos falsos, perdidos ou roubados



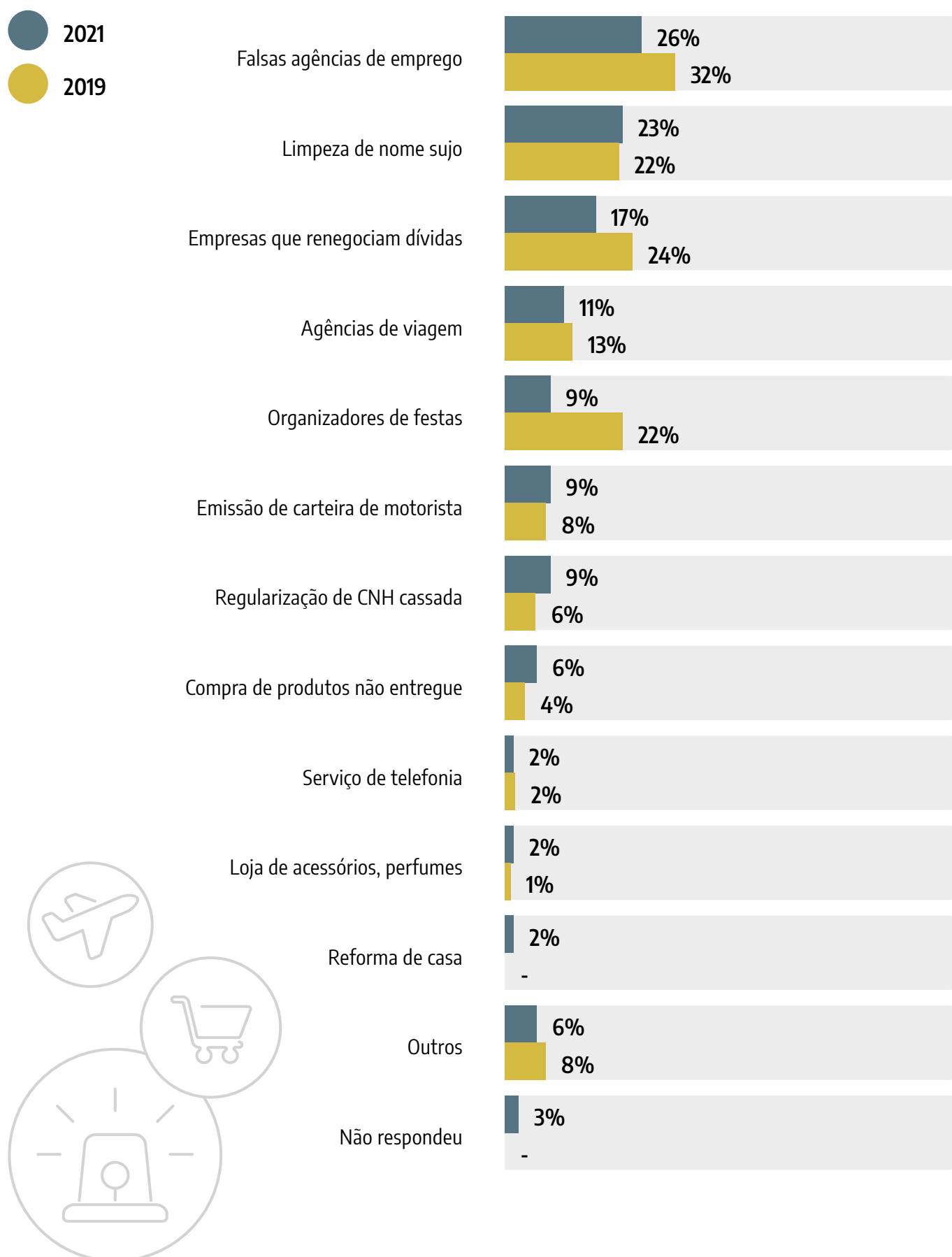
► Entre os serviços contratados, mas não realizados, as falsas agências de emprego se destacam



Da mesma forma que alguns bens não chegaram aos compradores, alguns serviços pagos não foram realizados: 12,2% mencionaram esse tipo de fraude. Entre esses consumidores, a ocorrência que mais se destacou foi o falso agenciamento de emprego, citado por 25,9%. Em seguida, aparecem os serviços de limpeza de nome sujo (23,3%) e de renegociação de dívida (17,2%). Agências de viagem e promotores de festa foram citados por, respectivamente, 11,2% e 8,6%. A emissão de carteira de habilitação e os serviços de regularização de CNH cassada

tiveram o mesmo percentual de 8,6%. Em tempos de crise, o desemprego aumenta e o endividamento das famílias sobe, fazendo com que aumente também a procura por serviços de recolocação profissional e renegociação, que se destacaram entre os contratados, mas não realizados. A ansiedade para resolver as pendências leva, por sua vez, a uma avaliação inadequada da empresa que presta o serviço, atrasando ainda mais a resolução da pendência. O consumidor pode negociar diretamente com o credor, que tem todo o interesse de receber.

Tipo de serviço contratado que não foi realizado



E a despeito de protocolos e investimentos em segurança adotados por bancos, 11,0% relatam transações financeiras como saques, pagamentos ou transferências na conta bancária sem a autorização. Para coibir esse tipo de fraude, recentemente, o Banco Central do Brasil

lançou uma ferramenta chamada “Registrato”⁵, onde os consumidores podem consultar suas informações de relacionamento bancário, como empréstimos, financiamentos, cadastramentos de chave PIX e aberturas de conta em seu nome.



Outras ocorrências usam brechas tecnológicas e engenharia social. A clonagem do número de celular e da conta de WhatsApp para solicitar depósitos aos parentes e amigos das vítimas foi mencionada por 10,9%. A lista de fraudes segue com outros ardis: emissão de cartão de crédito sem autorização usando documentos

falsos, perdidos ou roubados (8,7%), vendedores que enviaram o produto, mas não receberam o pagamento (7,4%) e tomada de crédito – empréstimos, financiamento ou crediário - sem autorização do entrevistado usando documentos falsos, perdidos ou roubados (7,1%) são outros exemplos.

⁵ <https://www.bcb.gov.br/cidadaniafinanceira/registrato>

► Maioria dos golpes foram realizados nas lojas on line



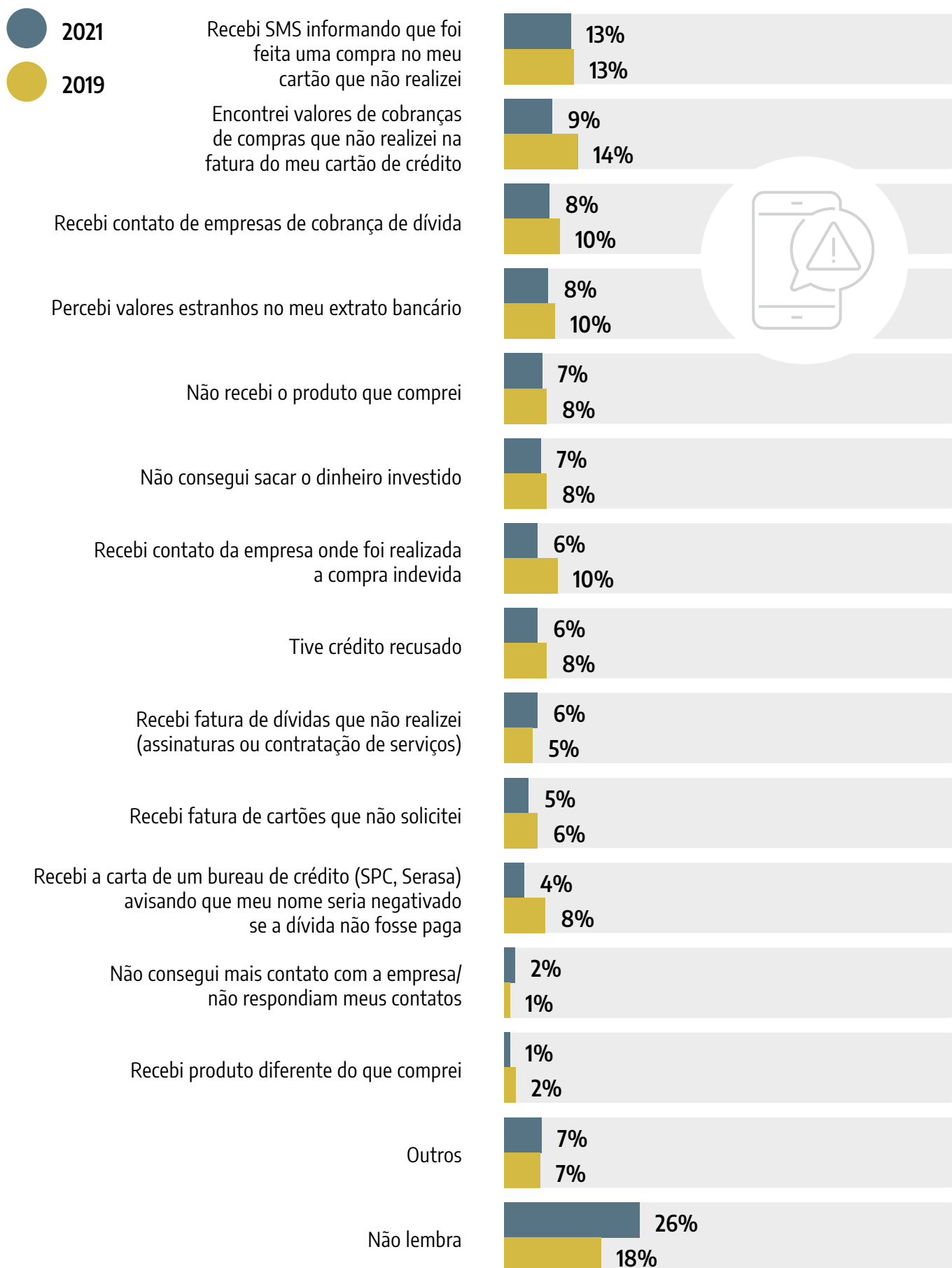
Os internautas vitimados por qualquer tipo de fraude foram indagados sobre o tipo de lugar onde o golpe aconteceu. Lojas online lideram a lista, citadas por 38,8%. Em seguida, aparecem os sites de compra e venda de produtos novos ou usados (15,0%). Bancos e financeiras foram citados por, respectivamente, 8,9% e 7,1%. Já as grandes lojas físicas foram citadas por 4,8%, enquanto o pequeno comércio foi mencionado por 3,9%.

A descoberta da fraude ocorreu principalmente através do recebimento de SMS informando compras no cartão de crédito que não foram realizadas pelo seu titular: 12,6% dos entrevistados souberam dessa forma que estavam sendo fraudados. A configuração de aplicativos para notificação de compras no cartão de crédito é uma ferramenta importante para que o consumidor possa solicitar o cancelamento da compra de forma mais célere. De acordo

com a pesquisa, 9,0% só descobriram compras indevidas no cartão quando receberam a fatura. Outras formas de descoberta mencionadas foram o contato de uma empresa de cobrança de dívidas (8,5%); o surgimento de valores estranhos no extrato bancário (8,3%); o não recebimento do produto comprado (7,2%) e a impossibilidade de sacar valores investidos (7,0%). Alguns consumidores relatam ainda que só souberam da fraude quando tiveram crédito negado (6,3%) e receberam o contato da empresa onde foi realizada a compra indevida (6,3%).

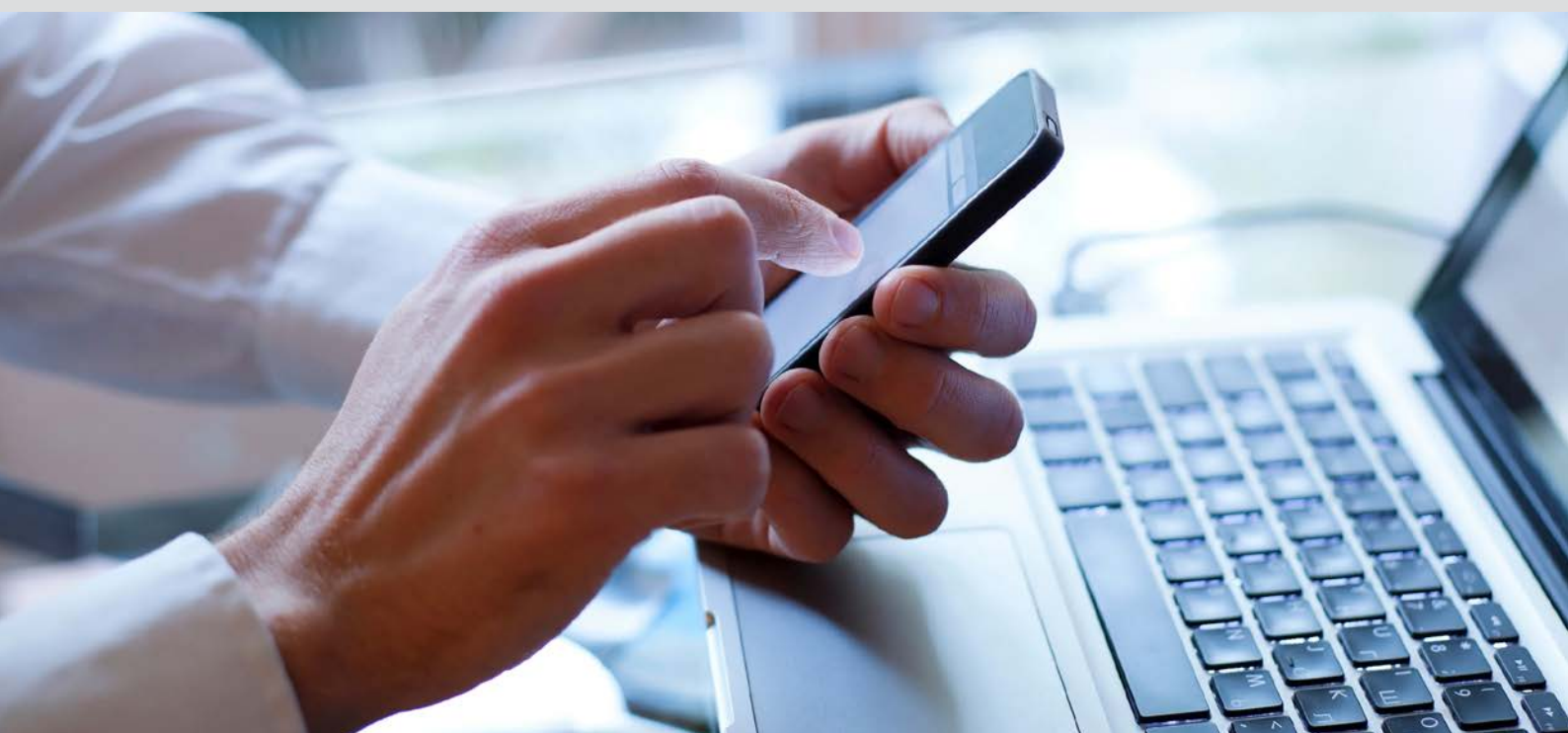
O estudo mostra que 35,6% imputam a fraude à ação de criminosos, sem que a empresa tenha tido responsabilidade direta. Além desses, 15,9% atribuem a fornecedores da empresa envolvida na fraude e 9,2% imputam a funcionários da empresa. 39,8% não souberam identificar ao certo quem cometeu a fraude.

Como descobriu que foi vítima de fraude



ANTECEDENTES E CONSEQUÊNCIAS DAS FRAUDES FINANCEIRAS

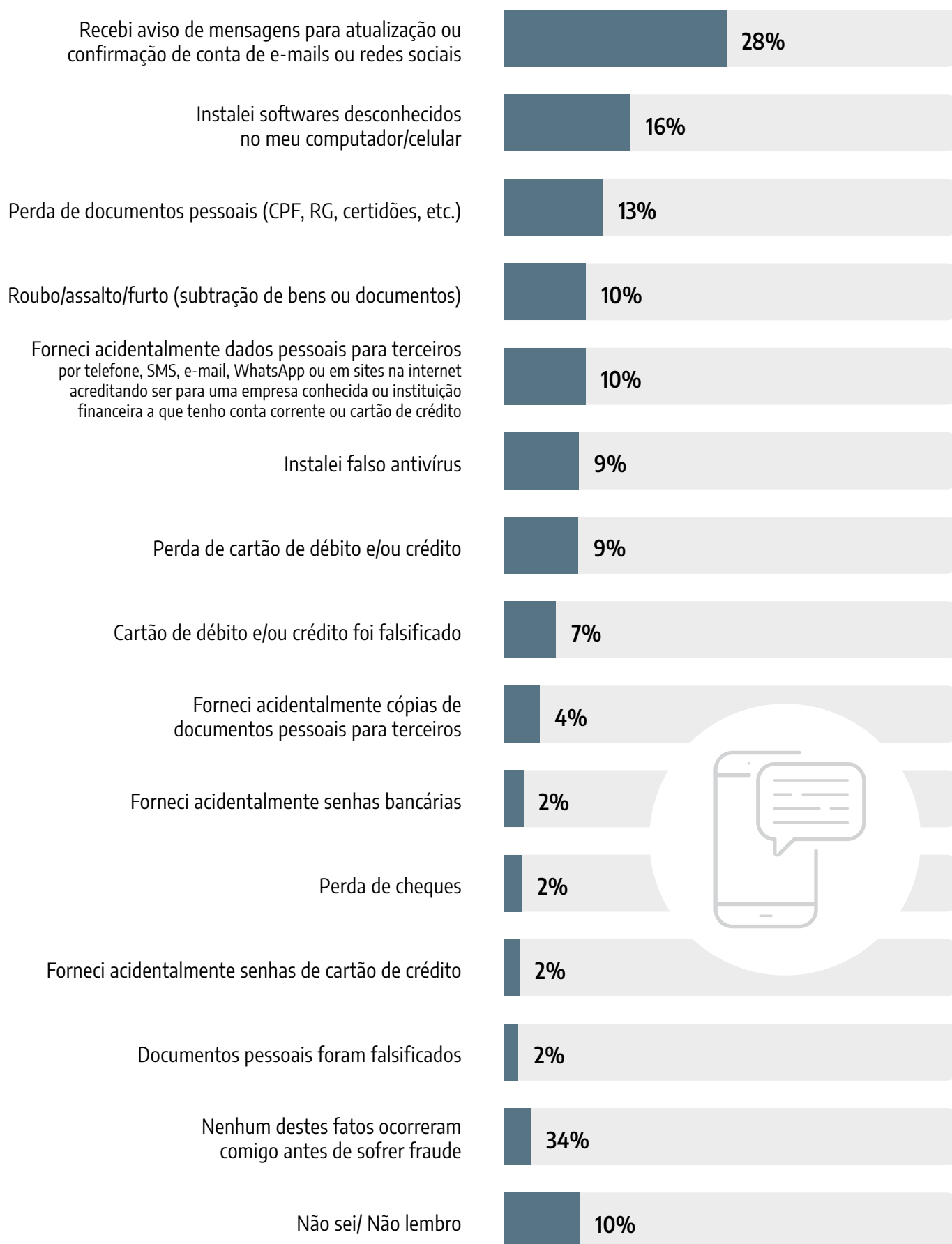
► Antes da fraude: atualização ou confirmação de conta de e-mail e redes sociais foi apontada como o principal fato antecedente, seguida da instalação de softwares desconhecidos e perda de documentos pessoais



Alguns comportamentos e acontecimentos aumentam a exposição às fraudes. Para compreender melhor esse fenômeno, o estudo indagou os entrevistados sobre fatos que antecederam o golpe. O precedente mais citado foi o recebimento de mensagens para atualizar ou confirmar conta de e-mail ou de redes sociais, mencionado por 28,2% dos entrevistados. Em seguida, aparece a instalação de softwares desconhecidos no computador ou celular (16,0%); a perda de documentos pessoais (12,6%), além de roubos e furtos, com a subtração de bens e documentos (10,4%). O fornecimento acidental de dados pessoais através de telefone, e-mail, SMS, WhatsApp ou

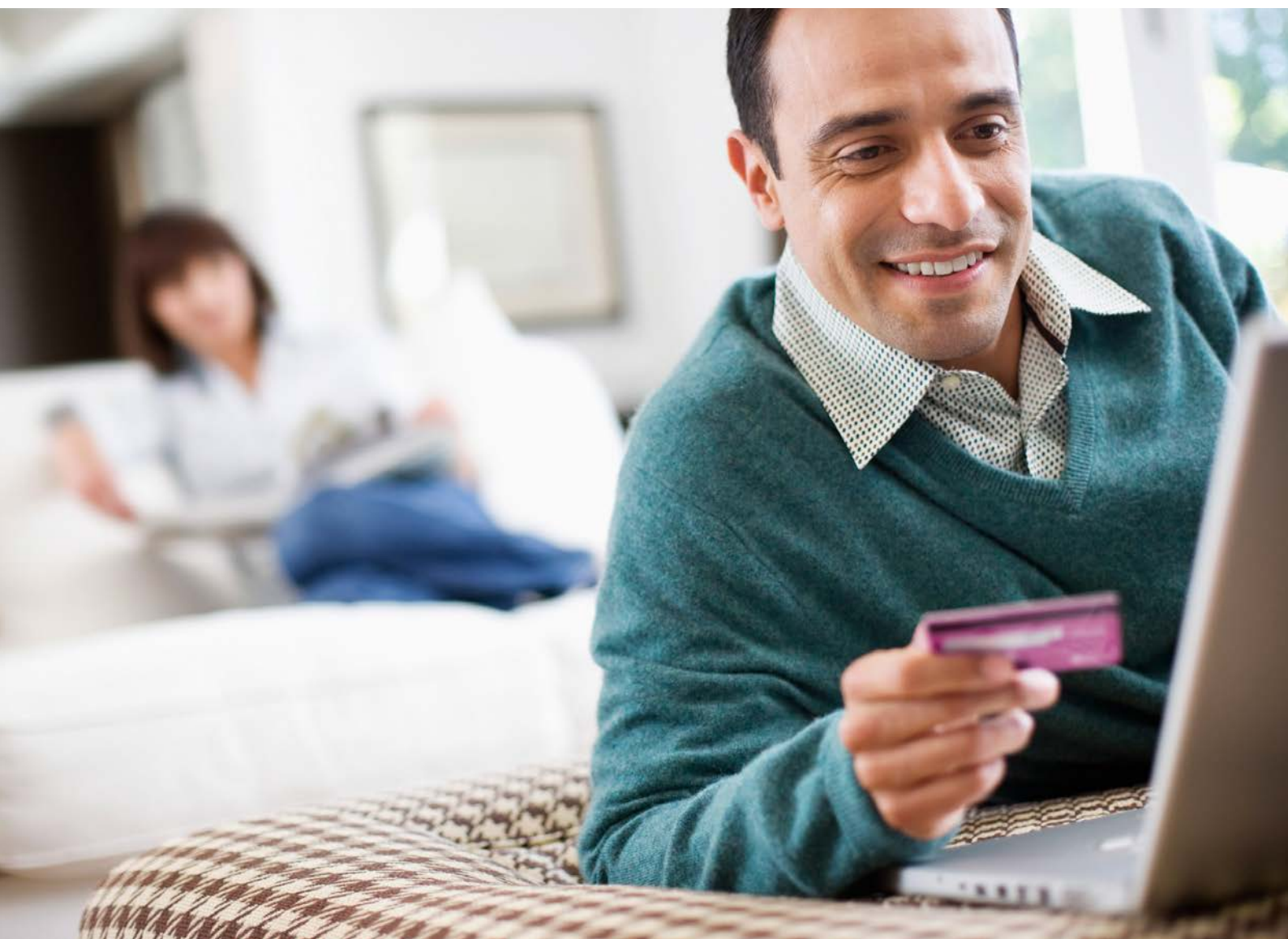
em sites na internet foi citado por 10,4%. A instalação de falso antivírus (9,5%), a perda de cartões de débito e de crédito (9,4%) e a falsificação desses cartões de débito e crédito (6,6%) também foram lembrados como fatos que precederam a fraude. Com percentuais menores, os entrevistados também citaram o fornecimento de cópias de documentos, senhas bancárias e de cartões para terceiros. Pouco mais de um terço (34,1%) responde, no entanto, que nenhuma das ocorrências listadas ocorreram antes da fraude, indicando que esses fatos não são uma condição necessária para o golpe.

Fatos que antecederam a fraude



Entre aqueles que ofereceram, inadvertidamente, informações pessoais a terceiros antes, a principal armadilha foi o cadastramento em sites falsos de promoção, citado por 26,0% desses entrevistados. O recebimento de falso e-mail de banco ou de empresas pedindo atualização cadastral foi lembrado por 21,3%. Também mereceu destaque o cadastramento em supostas

vagas de emprego (18,9%, com percentual ainda maior entre jovens e mulheres), além do contato telefônico de alguém fingindo ser funcionário de instituição financeira (16,0%). Outras menções foram a realização de compra em site falso (15,4%); a falsa notificação para quitação de débito financeiro, sob pena de ser processado ou negativado (14,5%), entre outras ocorrências.



As instituições financeiras alertam para o fato de que não solicitam senhas ou número de cartões através de ligação telefônica. Caso o consumidor se depare com esse tipo de abordagem, é recomendável que entre em contato com a sua agência ou call center. No caso dos sites falsos de promoção, mencionados em primeiro lugar quando se trata do compartilhamento inadvertido de

informações, é preciso exercitar sempre a desconfiança, checar a procedência e reputação da loja e não transmitir dados sensíveis. Sempre que houver a necessidade de compartilhar dados com alguém, como no caso do envio de um currículo, por exemplo, é preciso ter certeza de que, do outro lado, existe alguém de boa-fé – o que é facilitado pelas buscas na internet.

► Depois da fraude: 29% ainda não solucionaram o problema e um terço não tomou nenhuma medida para resolver



Uma vez ocorrida a fraude, 27,5% conseguiram resolver o problema em menos de um mês, ante 24,2% que levaram entre 1 mês e seis meses para resolver a situação. Além desses, 6,8% resolveram num prazo entre 7 a 12 meses, e 28,9% ainda não conseguiram resolver. Esse percentual aumentou 4 p.p na comparação com 2019, quando era de 24,5%.

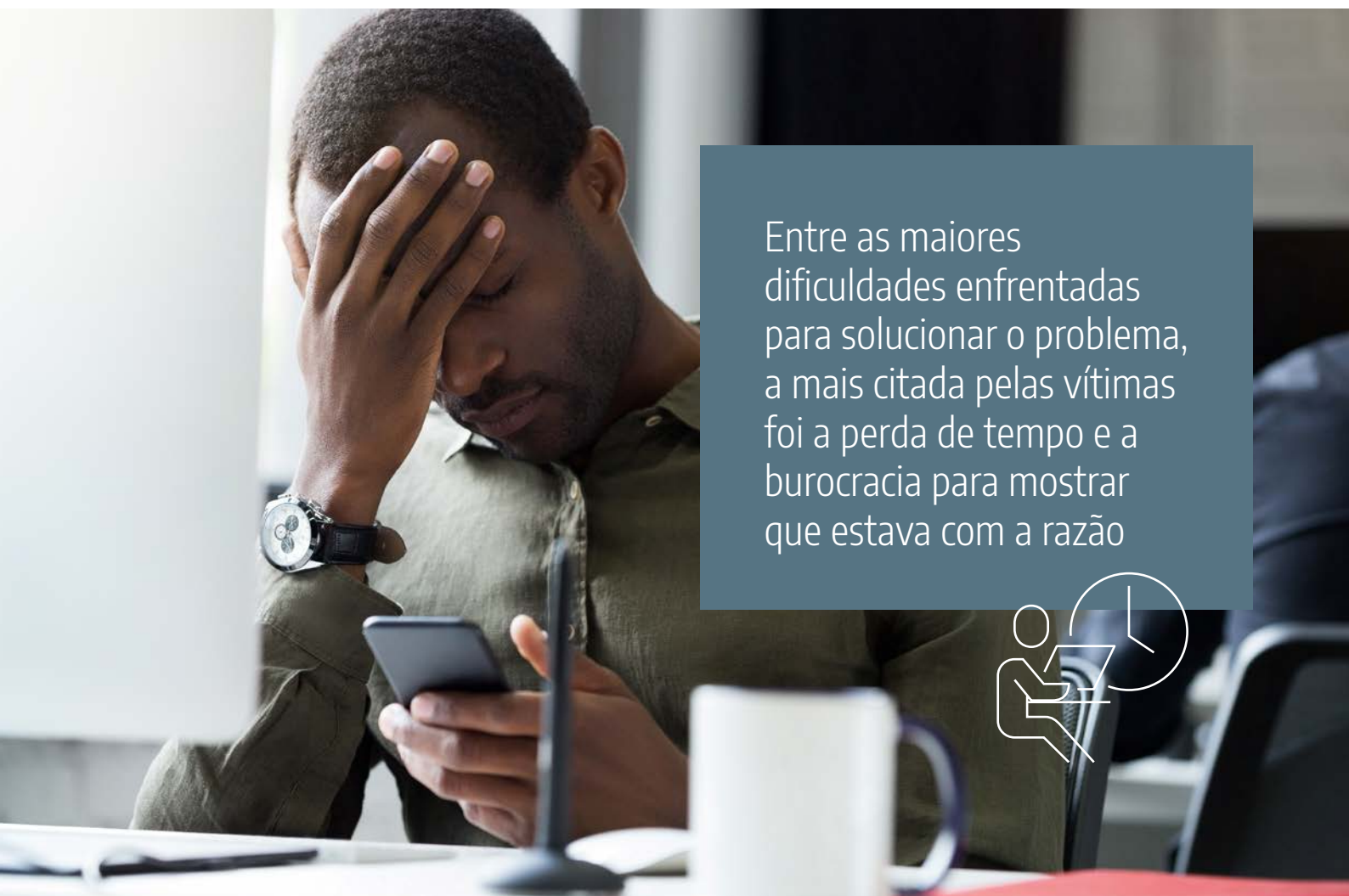
A pesquisa ainda aponta que 28,7% não tomaram nenhuma medida para solucionar o caso. Entre os principais motivos para a inércia, esses consumidores citam a baixa expectativa de que conseguiriam resolver o problema (44,9%); o fato de não saberem como fazê-lo (28,7%); e a escolha de não ter mais preocupações com o assunto (18,8%). Evitar vergonha e constrangimentos,

mesmo na condição de vítima da fraude, fez com que 9,6% desses internautas não agissem; 8,1% ainda mencionaram que empresa resolveu por própria iniciativa, sem que precisassem fazer algo.

Por outro lado, as principais medidas para solucionar a fraude foram o contato com o banco e administradora de cartão (26,6%); a negociação com a empresa ou instituição financeira para reaver valores ou reparar danos (17,9%); a abertura de boletim de ocorrência na polícia (16,1%). A procura de órgão de defesa do consumidor foi citada por 12,5%. Abertura de processo judicial e reclamação no Banco Central foram citadas por, respectivamente, 6,0% e 3,5%.

Entre aqueles entrevistados que agiram, houve queda na utilização de canais offline para a resolução da fraude: 58,3% citaram esse tipo de canal, ante 65,8% em 2019. O canal offline mais citado foi a conversa telefônica (41,8%), seguida pela comparecimento na empresa (13,0% em 2021, ante 20,9% em 2019), e pela notificação judicial

(6,8%). Entre os canais online (50,5%), o e-mail foi citado por 34,4% daqueles que buscaram resolver a situação. Cresceu, nesse meio, o percentual de consumidores que citaram o WhatsApp, passando de 11,8% em 2019 para 16,5% em 2021. As redes sociais foram citadas por 11,4% desses entrevistados.



Entre as maiores dificuldades enfrentadas para solucionar o problema, a mais citada pelas vítimas foi a perda de tempo e a burocracia para mostrar que estava com a razão

Entre as maiores dificuldades enfrentadas para solucionar o problema, a mais citada pelas vítimas de fraude foi a perda de tempo, lembrada por 44,6%. Em seguida, apareceram a burocracia para mostrar que a vítima estava com a razão (27,0%); a perda de dinheiro (25,9%); e a falta de conhecimento sobre quem poderia resolver o caso (20,4%). Além desses, 19,0% relatam que não houve dificuldade para a resolução do problema – percentual que cresceu 4 p.p. na comparação com 2019 (14,6%).

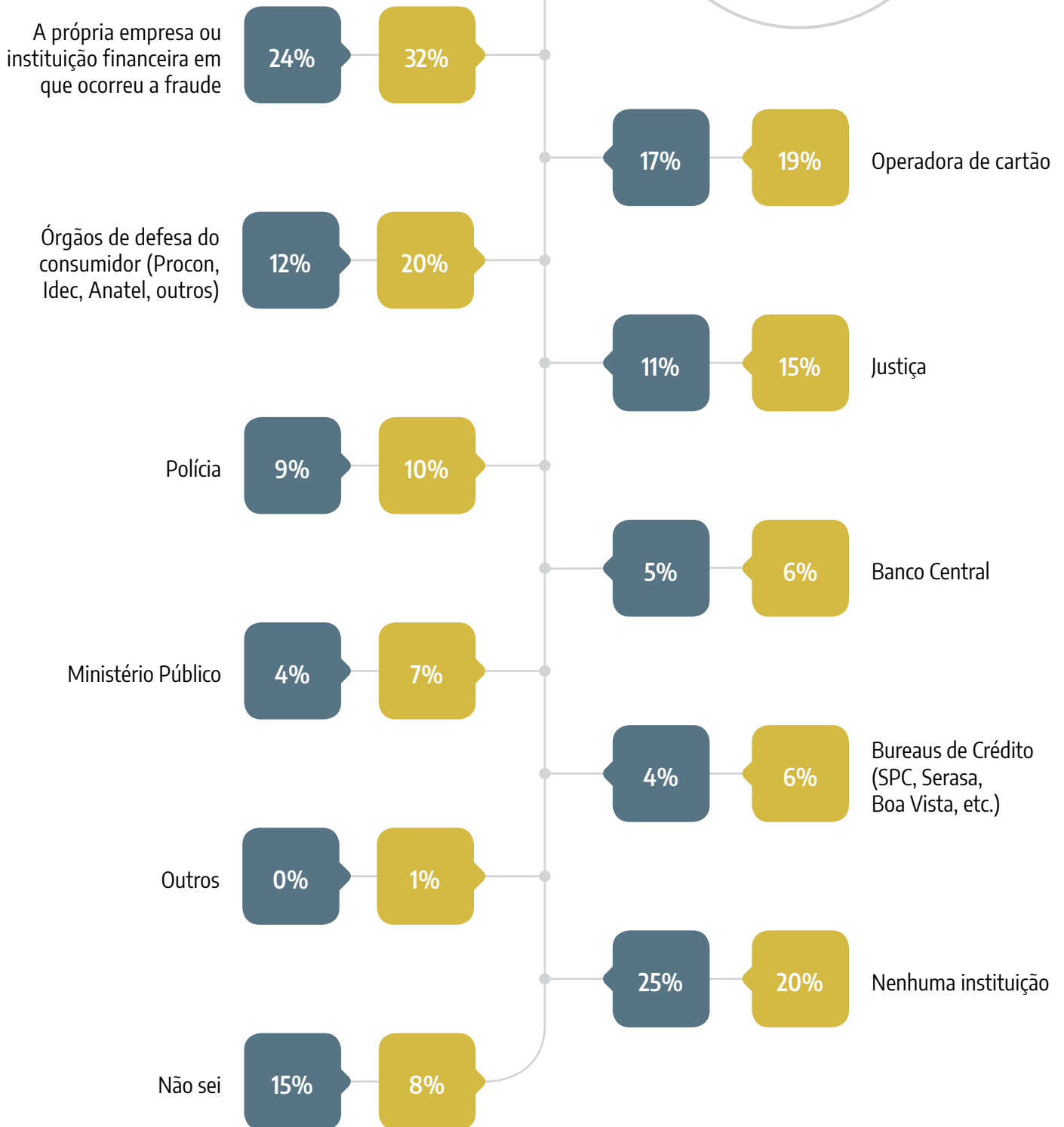
Questionados sobre quais instituições contribuíram para

a resolução do caso, 23,6% dos entrevistados citaram a própria empresa onde ocorreu a fraude, 16,8% citaram a operadora de cartão e 12,1% mencionaram órgãos de defesa do consumidor – nos três casos, observou-se percentuais maiores entre os entrevistados das classes A e B. Além dessas instituições, foram citadas a Justiça (11,5%), a Polícia (9,5%), o Banco Central (5,0%), o Ministério Público (4,0%) e os Bureaus de Crédito (3,9%). Ainda segundo a pesquisa, 25,0% não contaram com a contribuição de nenhuma instituição.

Instituições que contribuíram para a resolução do caso



● 2021
● 2019



► R\$ 2,7 bilhões é o prejuízo decorrente de fraudes financeiras nos últimos 12 meses



As fraudes podem deixar consequências materiais e imateriais. De acordo com o estudo, metade dos entrevistados tiveram prejuízos financeiros (50,4%), ainda que num segundo momento alguns tenham conseguido reverter a perda. E além dos prejuízos ocasionados pela própria fraude, 20,9% dos entrevistados relataram custos para resolver o problema. Entre esses custos, os principais foram os gastos com deslocamento (43,4%); os gastos com chamadas telefônicas (38,9%); e o pagamento de taxas (32,8%) e advogados (26,3%). Os entrevistados ainda citaram gastos com estacionamento (23,7%), com cartório (19,7%) e materiais de escritório (16,7%).

Considerando-se os custos incorridos para a resolução do problema e as perdas ocasionadas pela própria fraude, para quem os teve, o valor médio do prejuízo foi de R\$ 512,4, sendo que 19,7% mencionaram um valor acima de R\$ 800. Com esses valores, estima-se que o prejuízo decorrente de fraudes financeiras sofridas no universo dos internautas brasileiros chegou a R\$ 2,7 bilhões, incluídos os gastos na busca de reparação do problema.

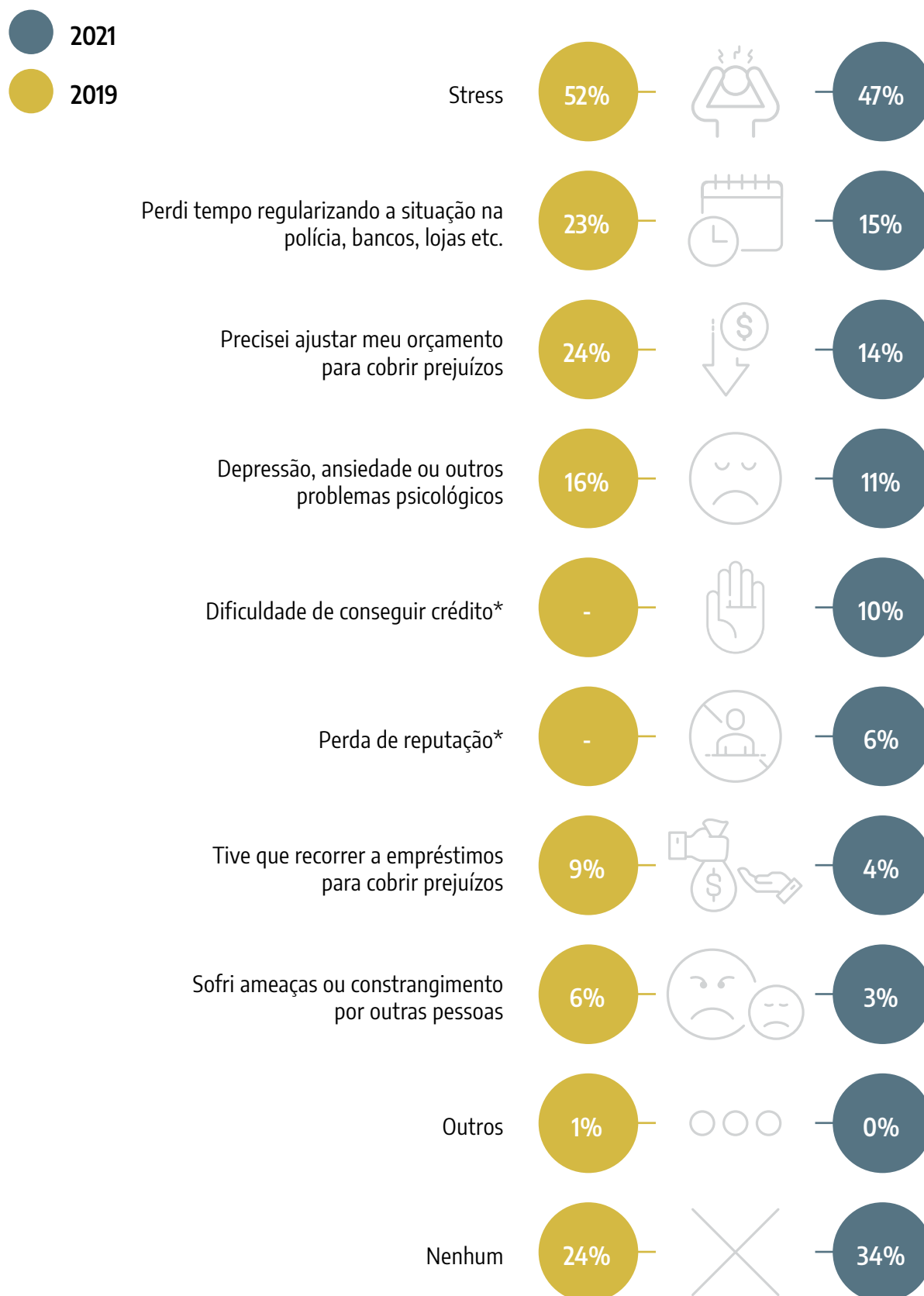
De acordo a pesquisa, 65,3% conseguiram recuperar ao menos uma parte do que perdeu, sendo que 43,2% recuperaram todo o valor. Esse percentual cresceu 11 p.p.

na comparação com o observado em 2019 (32,2%). 22,1% recuperaram parte do valor total, ante 34,1% em 2019. Já o percentual dos que não conseguiram recuperar nenhuma quantia ficou estável: 34,7%, em 2021, ante 33,8% em 2019. Mais da metade dos consumidores que ainda não recuperaram o prejuízo total tampouco espera recuperar o que foi perdido (53,1%), embora uma parte (46,9%) ainda tenha esperança.

Não bastasse a perda de dinheiro, alguns ainda tiveram que lidar com o constrangimento de ficar com o nome sujo em razão da fraude. Segundo a pesquisa, 19,3% dos internautas vítimas de fraude foram incluídos nos cadastros de devedores, sendo que 12,0% conseguiram resolver e 7,3% ainda permanecem com restrição no nome. Além desses, 73,6% relatam que não chegaram a ser negativados e 7,2% não souberam dizer.

Os danos também são emocionais: 46,9% relataram ter sofrido stress por causa da fraude. Além disso, 15,1% citaram a perda de tempo; 13,7% mencionaram ajustes no orçamento para cobrir os prejuízos e 11,5% relataram depressão, ansiedade e outros problemas psicológicos, além da dificuldade para conseguir crédito (9,8%).

Outros prejuízos sofridos devido à fraude



* Respostas pré-codificadas inseridas em 2021

PERCEPÇÕES SOBRE AS FRAUDES

► Lições aprendidas e percepções sobre as fraudes: 62% dos entrevistados consideram-se mais preparados para evitar novos golpes



Depois de terem passado pelas consequências de uma fraude, 61,9% dos entrevistados se consideraram mais preparados para evitar esse tipo de crime (percentual que chega a 66,8% entre os homens), ante 38,1% que ainda se sentem vulneráveis. Essa experiência também fez com que a grande maioria adotasse medidas para evitar novos golpes. De acordo com a pesquisa, 39,1% já não respondem e-mails ou telefonemas solicitando informações pessoais; 36,7% não abrem mensagens -- SMS, WhatsApp, e-mail, privadas nas redes sociais -- de desconhecidos e suspeitos; 36,6% só fazem compras em locais confiáveis e 36,4% não compartilham dados pessoais em rede social. Além dos cuidados com dados, 35,1% mencionam pesquisa sobre a reputação das lojas antes de efetuar a compra,

33,5% acompanham com frequência a fatura do cartão de crédito e 33,7% o extrato bancário; 32,6% verificam se as páginas da internet possuem conexão segura; 29,6% evitam compras em sites que vendem com preços muito abaixo do mercado e 28,5% checam a veracidade de boletos recebidos por e-mail.

A fim de mapear os hábitos e comportamentos dos entrevistados, a pesquisa mediu o grau de concordância dos internautas vítimas de fraude com algumas frases, constatando que 80,4% já deixaram de comprar em um site por desconfiar de sua honestidade. Percentual elevado também concordou com a afirmação de que pessoas ingênuas são mais propensas a fraudes (79,5%). A maior

parte (73,2%) também acredita que os fraudadores estão sempre um passo à frente das medidas de segurança. A noção de que pessoas gananciosas estão mais sujeitas a fraudes teve a concordância de 69,4%. Para 68,7%, esse também é o caso das pessoas que vivem em situação de necessidade ou urgências de dinheiro. Todas essas frases

obtiveram um índice de concordância acima do observado na pesquisa de 2019. Além disso, mas não menos importante, apenas 35,6% concordaram que confiam nos sistemas de proteção contra fraudes das empresas – percentual que também cresceu na comparação com 2019.



Instituições financeiras são vistas como os principais responsáveis para evitar que os consumidores sejam vítimas de fraudes



Quem são os responsáveis, afinal, por criar medidas a fim de evitar que os consumidores caiam vítimas de fraudes? Para 71,0%, as instituições financeiras estão entre os responsáveis. 66,2% mencionaram ainda os órgãos reguladores, como a CVM e o Banco Central e 64,3% citaram a Política Federal. Os próprios consumidores também se destacaram, sendo lembrados por 60,8%, além de lojistas (58,8%), entre outras instituições.

O compartilhamento de dados aparece como algo sensível na percepção dos entrevistados – e da sociedade de maneira geral, tendo ensejado recentemente a criação de um marco

regulatório, a Lei Geral de Proteção de Dados. De acordo com a pesquisa, 93,6% consideraram que a exposição de informações em redes sociais é uma prática que contribui, em alguma medida, para que alguém sofra uma tentativa de fraude, e 92,8% consideraram que o excesso de dados que as empresas coletam de consumidores também dá a mesma contribuição. A maneira como os dados são armazenados por empresas, as falhas de segurança dos computadores e o excesso de dados que o governo coleta dos consumidores foram considerados da mesma forma por mais de 90% dos consumidores.

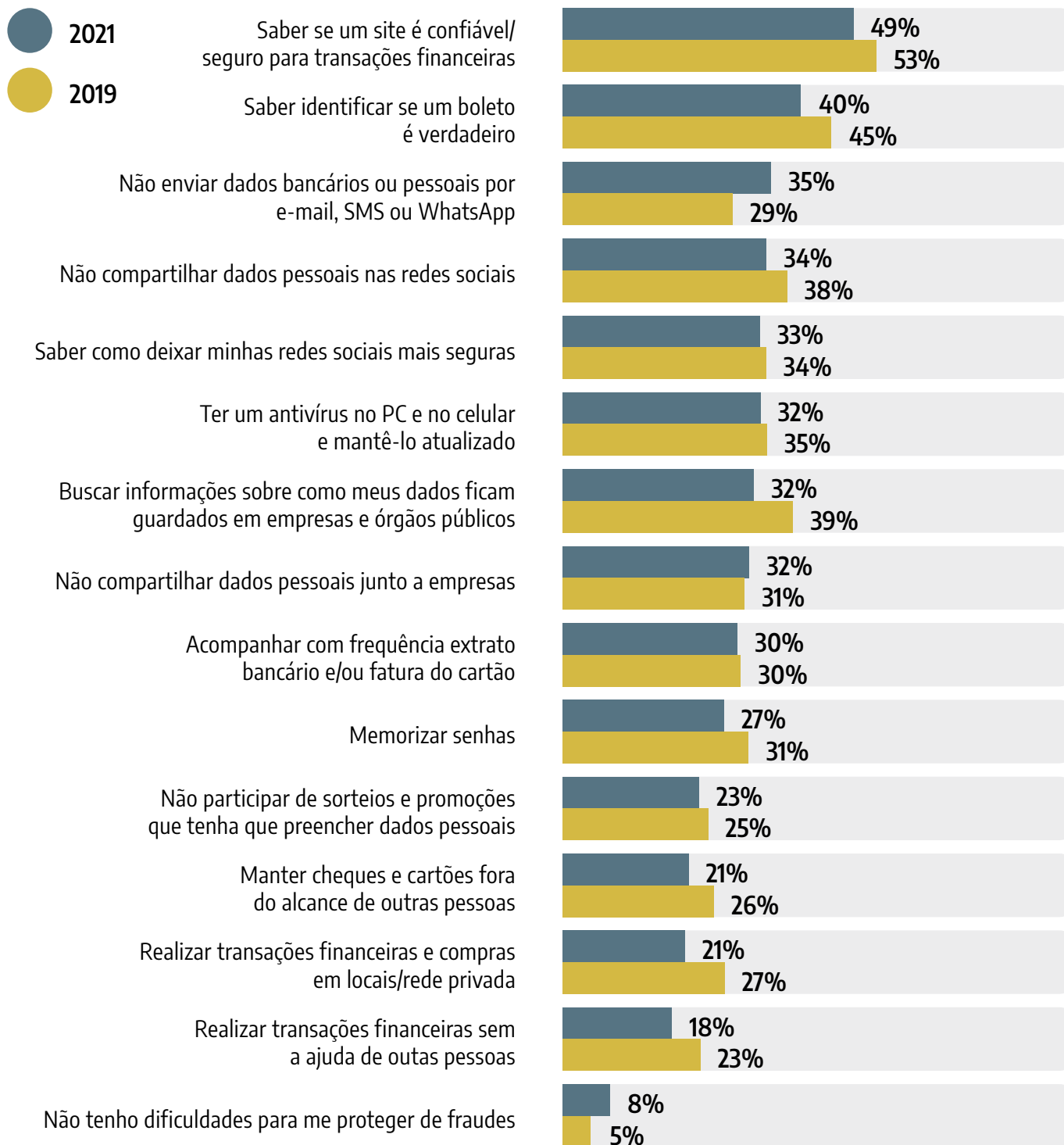
► Serviço de notificação sobre movimentação no CPF é visto como principal medida de proteção dos consumidores a fraudes



No rol das medidas que poderiam contribuir para proteger os consumidores contra fraudes, os serviços que notificam o consumidor sobre movimentações de seu CPF foram os mais citados (68,3%). 62,9% mencionaram ainda o aviso, por parte das instituições financeiras, sobre as transações em seu nome. Também mereceu destaque o uso da biometria (56,6%) e a validação de transações por parte de instituições financeiras (56,2%), para além da notificação; a consulta de CPF em cadastros de proteção ao crédito (46,9%); e o uso de certificado digital (44,2%).

Entre as dificuldades mencionadas para se proteger contra as fraudes, 49,3% dos entrevistados citaram a verificação sobre a confiabilidade de um site para transações financeiras. Outra dificuldade prática destacada foi a verificação sobre a veracidade de um boleto (40,3%). O não envio de dados bancários e pessoais por e-mail, SMS ou WhatsApp (35,3%) e o não compartilhamento de dados pessoais nas redes sociais (34,5%) também foram lembrados. Entre outras dificuldades, cerca de um terço dos entrevistados mencionaram a dificuldade de saber como deixar as redes sociais mais seguras (33,4%).

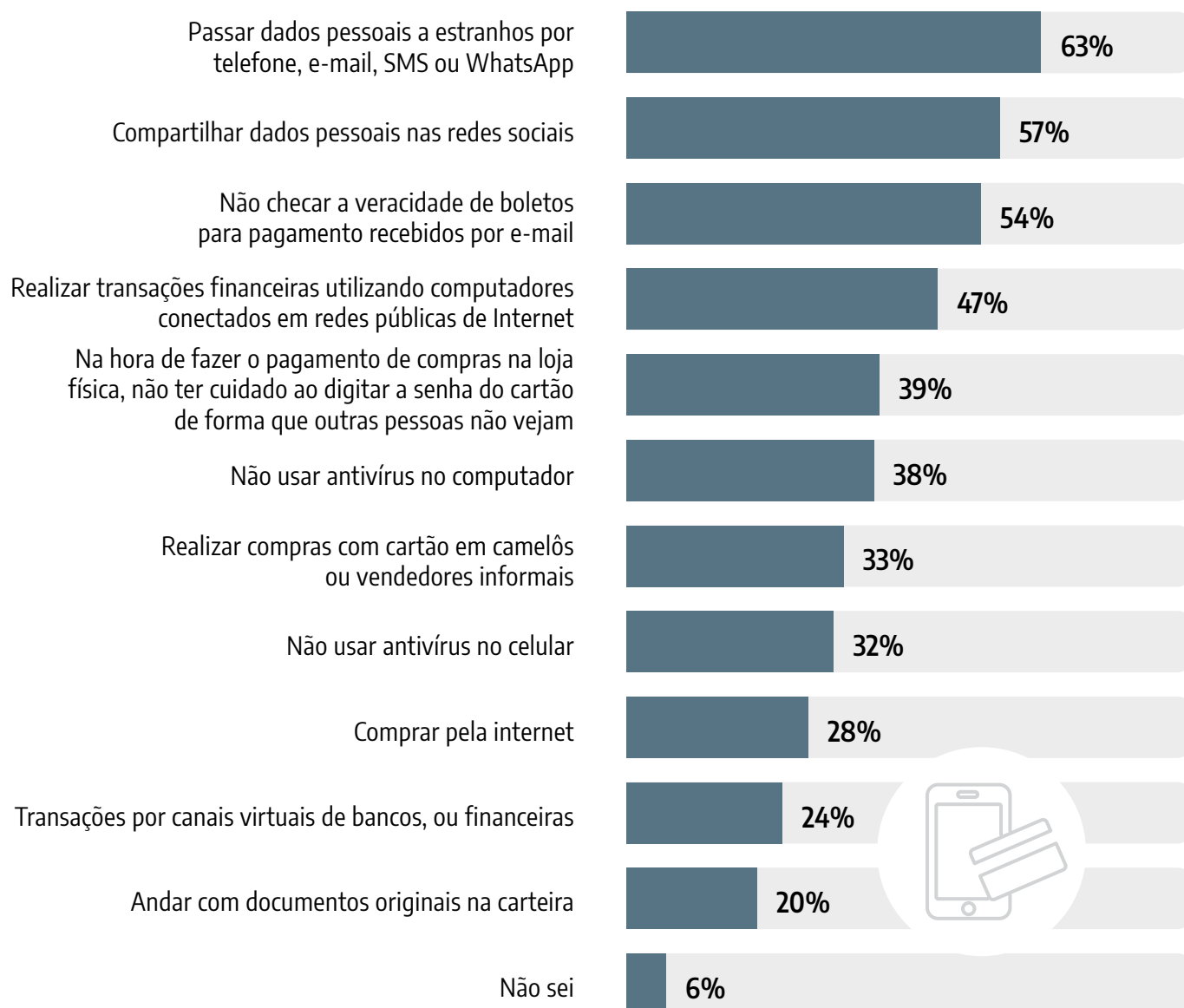
Principais dificuldades para se proteger de fraudes



A pesquisa elencou o que, na avaliação dos internautas que sofreram fraude nos últimos 12 meses, deixa as pessoas mais suscetíveis a esse tipo de ocorrência. 63,2% mencionaram o compartilhamento de dados pessoais a estranhos através de telefones e mensagens; 56,9% citaram o compartilhamento desses dados em redes sociais;

e 54,0% lembraram da não verificação de autenticidade de boletos recebidos. Outras suscetibilidades apontadas foram a realização de transações financeiras em redes públicas de internet (47,4%); a falta de cuidado ao digitar senhas em lojas físicas (38,6%); o não uso de antivírus no computador (37,7%), entre outros.

Situações que deixam as pessoas mais suscetíveis a fraudes



Por fim, entre as situações vividas pelas vítimas de fraude ao longo dos últimos 12 meses, o desemprego foi a que mais se destacou, citada por 32,9%, seja acometendo o próprio entrevistado, seja acometendo alguém da família. Além do drama do desemprego, 27,0% contam que ficaram com muitas dívidas pendentes, 13,6% mencionam que ficaram acamados ou muito doentes, 9,0% relatam o recebimento de dinheiro da venda de algum bem e 6,5% se divorciaram. Essas situações servem de alerta para os casos de fraudes e demandam especial cuidado de quem as vivencia, pois exigem trânsito de documentação e dados.

A pesquisa ainda mostra que, se nem todos caíram num golpe de ligação ou mensagem, 84,1% receberam um contato através desses meios que pareceu suspeito. Além desses, 10,0% não perceberam essa abordagem e 5,9% não se lembram. E mesmo os programas sociais criados em meio à pandemia foram vistos como oportunidade para fraudadores: de acordo com o estudo, 22,6% dos entrevistados receberam mensagem falsa para cadastro no programa de Auxílio Emergencial do Governo Federal, o que mostra que a vulnerabilidade às fraudes aparece em todas as classes e condições sociais.



O futuro será cada vez mais digital. Depois do crescimento das compras online e das transações bancárias pela internet – tendência reforçada, aliás, pela pandemia –, inicia-se um novo tempo para os meios de pagamento instantâneos. Essas transformações prometem reduzir os custos de transação e representam um grande potencial econômico.

Para cada nova solução, surgirão novas modalidades (ou tentativas) de fraude, mas isso não é motivo para barrar o bom uso da tecnologia. A nova realidade requer investimentos em ferramentas de segurança e a disseminação da educação digital, de modo a prevenir a

ocorrência fraudes e a evitar todas as consequências e transtornos relatados ao longo da pesquisa. A identificação e punição de fraudadores também é um passo importante para aumentar os custos do crime.

Numa época em que os dados pessoais não estão totalmente em nosso controle, mesmo sem que o consumidor saiba ou permita, existe a possibilidade de vazamento de informações cadastrais ou tributárias, tanto no ambiente das empresas privadas quanto dos órgãos públicos. Assim, é importante adotar procedimentos mais seguros e evitar certas atitudes, como nas situações a seguir.



Ao constatar a perda de documentos pessoais

(RG, CPF, habilitação, título de eleitor etc.)

Registrar um boletim de ocorrência imediatamente, pois, como mostra a pesquisa, os dados pessoais podem ser utilizados em uma série de ações criminosas, como as compras não autorizadas, por exemplo. Também é importante solicitar o mais rápido possível o bloqueio de cartões de banco, de lojas e talões de cheque.



Nas compras virtuais

Além de verificar os preços, é importante dar preferência às lojas e sites mais conhecidos; o consumidor sempre deve procurar garantias e saber mais sobre a reputação da loja/vendedor, pois os rankings ajudam a identificar vendedores suspeitos. Outra medida de proteção é consultar o certificado de segurança da loja, geralmente localizado no rodapé na página. Ele garante que o site possui barreiras contra o ataque de hackers, infecção por malwares⁶ e clonagem de dados.



Ao lidar com boletos bancários

Por ser prático e acessível, o boleto bancário é um meio de pagamento bastante utilizado pelos brasileiros. Muitos fraudadores enviam cobranças com código de barras via correio, SMS, e-mail ou WhatsApp, simulando compromissos financeiros comuns dos consumidores, que acabam pagando a conta sem perceber. Por isso, antes de realizar o pagamento, é importante verificar atentamente as informações, sobretudo o valor e os dados do beneficiário. Caso seja comprovada a falha nos sistemas de cobrança de um banco ou loja, por exemplo, a responsabilidade não será do consumidor e ele deve ser ressarcido.



Ao constatar despesas não autorizadas no cartão de crédito ou débito

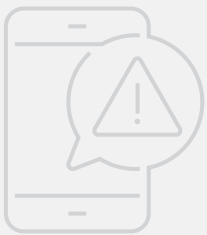
Nessas situações o consumidor deve entrar em contato imediatamente com a empresa emissora do cartão para comunicar que os gastos não foram feitos por ele. Também é válido registrar boletim de ocorrência e adotar algumas medidas de precaução, como jamais digitar senha do cartão em compras on-line (os sites não precisam dela para efetivar a transação), nunca acessar o internet banking em lan houses, computadores ou dispositivos que não pertençam ao usuário e sempre conferir a fatura para verificar despesas, mesmo que de menor valor.

⁶ Programas ou códigos maliciosos que podem infiltrar-se em sistemas de computação de maneira indevida para roubar dados ou causar danos.



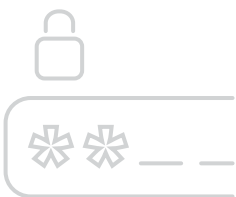
Ao constatar movimentação financeira atípica

O correntista deve imediatamente recorrer ao banco para buscar o ressarcimento e outras ações corretivas. Ao mesmo tempo, é importante estar atento aos hábitos de navegação, evitando clicar em mensagens de promoções, descontos, oportunidades de investimento e outros serviços bancários. As instituições são extremamente rígidas em relação à segurança virtual, e não enviam instruções por e-mail. O recomendável, diante de um link suspeito, é jamais clicar e, assim que possível, entrar em contato com o banco para esclarecer a dúvida.



Cuidados com os aplicativos de mensagem

Para evitar a clonagem do WhatsApp, a recomendação é, em primeiro lugar, não informar a terceiros códigos recebidos por mensagem, a menos que tenha absoluta certeza do que se trata. Em geral, o código fornecido possibilitará que o criminoso acesse seus contatos a partir de outros dispositivos. Outra recomendação é ativar a chamada verificação em duas etapas nas configurações do aplicativo. Através dessa verificação, você irá cadastrar uma senha, que será solicitada nas tentativas de uso do seu número em outros dispositivos. No caso do WhatsApp, também é importante cadastrar um e-mail seguro para que você possa recuperar a sua senha de verificação, caso se esqueça.







Ao definir e usar uma senha

É importante elaborar boas senhas, não utilizando informações óbvias como a data de aniversário ou o nome e evitar o uso de uma mesma senha para vários acessos. Também é recomendável trocar a senha periodicamente. Além disso, ao digitar uma senha em ambiente presencial, certifique-se de que ninguém esteja observando.



► Metodologia

PÚBLICO-ALVO	MÉTODO DE COLETA	TAMANHO AMOSTRAL	DATA DE COLETA
 <p>Pessoas residentes em todas as capitais do país, homens e mulheres, com idade igual ou maior a 18 anos, das classes econômicas ABC (excluindo analfabetos).</p>	 <p>Pesquisa realizada via web.</p>	 <p>949 casos e pós ponderada considerando as capitais do país, sexo, idade, classe social e escolaridade, gerando uma margem de erro no geral de 3 p.p para um intervalo de confiança a 95%.</p>	 <p>15 de abril a 30 de abril de 2021.</p>



Sistema CNDL

