FRAUDES NO BRASIL 2025

Estudo completo sobre ameaças e soluções.

REALIZAÇÃO

QITECH

Em um cenário global, em que a digitalização avança de forma acelerada, a prevenção e a detecção de fraudes se tornaram temas críticos para as instituições financeiras. Como especialista em KYC e antifraude, acredito que os insights sobre as tendências, desafios e estratégias de combate às fraudes deste material podem apoiar empresas a tornarem toda sua jornada mais segura.

O ano de 2024 destacou-se por um aumento significativo nas tentativas de fraude, impulsionadas pela sofisticação das tecnologias utilizadas por cibercriminosos e pela crescente vulnerabilidade decorrente da integração digital. Este relatório visa não apenas descrever os tipos de fraudes mais comuns, mas também fornecer uma análise aprofundada das metodologias utilizadas pelos fraudadores, as falhas exploradas nos sistemas de segurança e as melhores práticas adotadas pelas empresas para mitigar esses riscos.

A QI Tech, que oferece soluções tecnológicas para o setor financeiro, reafirma seu compromisso com a inovação e a segurança, buscando constantemente aprimorar suas tecnologias e metodologias para proteger seus clientes e o mercado como um todo.

Boa leitura,
Ricardo Alfaro, sócio da QI Tech.

Ricardo Alfaro é Partner na QI Tech, onde atua desde 2022. Com formação em Engenharia Mecânica pela Universidade Federal do Paraná, Ricardo tem uma carreira marcada por liderança em vendas e transformação de mercados. Ele traz uma sólida experiência em tecnologia, segurança e experiência do cliente, destacando-se no mercado de antifraude e compliance no Brasil.

Índice

1. Panorama de fraudes no Brasil em 2025 3

a. Deepfake 4
i. A tendência dessa fraude 6

b. Fraudes em pagamentos digitais 7
i. A tendência dessa fraude 9

c. Identidades falsas 11
i. A tendência dessa fraude 13

d. Invasão de contas bancárias 14
i. A tendência dessa fraude 16

2. Soluções de mitigação de fraude QI Tech 18

a. Onboarding 19
i. Validação cadastral 20
ii. Análise de documentos 20
iii. Reconhecimento facial 21
1. Captação 21
2. Análise 22
3. Reconhecimento 23
iv. Device scan 23
v. Motor de crédito 23

b. Análise de crédito 24

c. Antifraude transacional 25

d. QI Sign – assinatura eletrônica com reconhecimento facial 27

3. Sobre a QI Tech 28

4. Referências 29

Panorama de fraudes no Brasil em 2025

A digitalização é um processo global que atinge os mais variados setores, especialmente depois da pandemia de Covid-19. Em 2022, **84,9% das empresas brasileiras de médio e grande porte utilizaram ao menos uma tecnologia digital avançada**, segundo o IBGE.

Num contexto em que o mundo dos negócios começa a se mesclar com o mundo digital, diversas oportunidades surgem para empresas ao redor do mundo. Contudo, esse progresso tecnológico também traz consigo ameaças, sendo as mais significativas as fraudes e golpes.

Conforme a Associação de Examinadores Certificados de Fraude, cerca de **5 trilhões de dólares são perdidos globalmente por golpes fraudulentos**. No Brasil, isso não é diferente. No primeiro semestre de 2023, o **Brasil havia reportado 2.800 tentativas de fraude por minuto**, sendo o terceiro país com maior risco de fraude no mundo.

Isso evidencia uma realidade: As fraudes estão em crescendo e se proliferando rapidamente.

Existem diversos tipos de fraude, que variam desde o setor em que o golpe está sendo aplicado até como ele é realizado. **Em 2023, os principais tipos de fraude foram:**

- **Deepfakes;**
- **Fraudes em pagamentos digitais;**
- **Identidades falsas;**
- **Invasão de contas bancárias.**

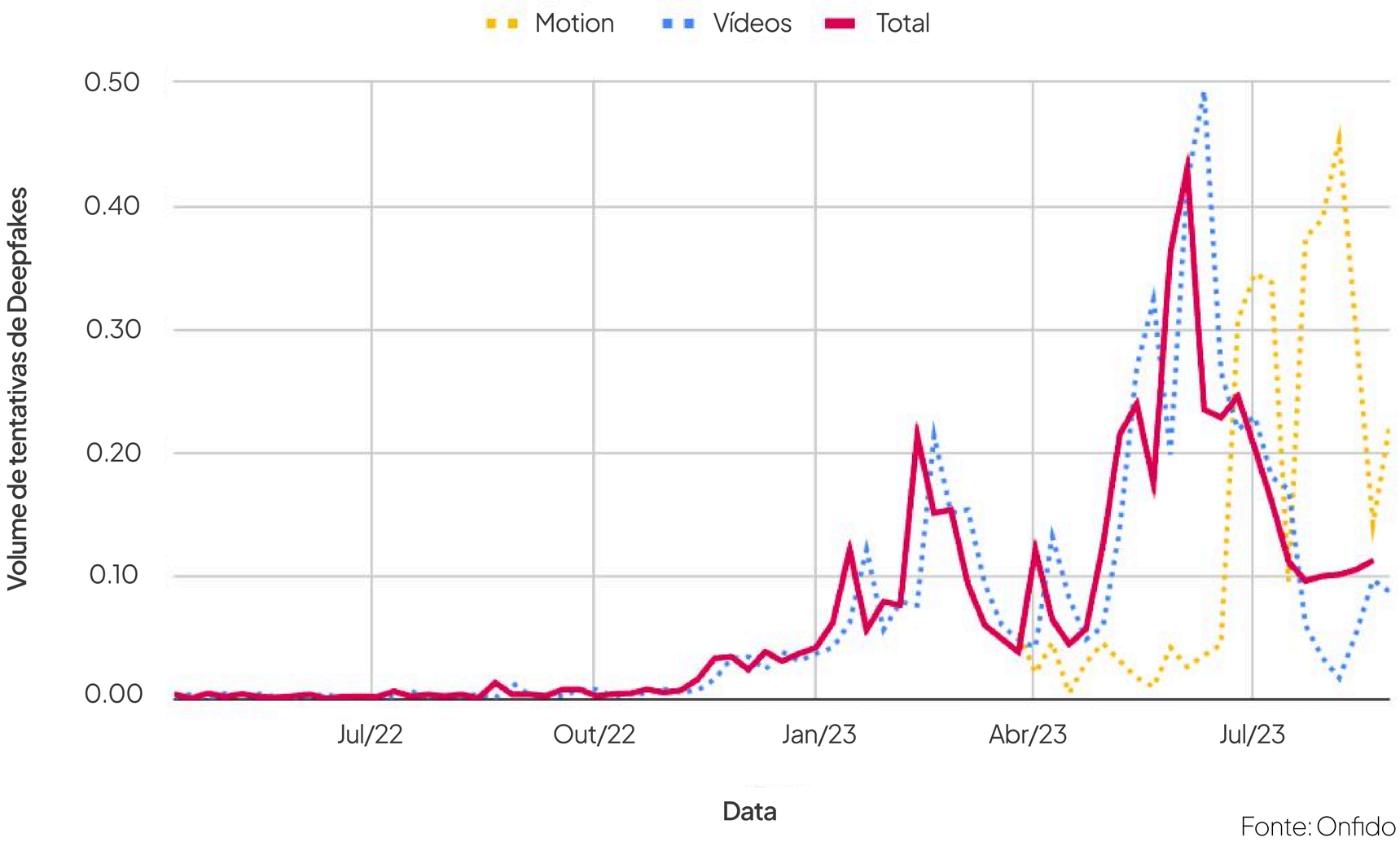
Trataremos sobre todas essas temáticas.

Deepfakes

Deepfakes são imagens ou vídeos digitalmente manipulados que **alteram o rosto de alguém,** fazendo com que uma pessoa se pareça com outra. Além disso, essa tecnologia também é aplicada em áudios, **modificando a voz da gravação para enganar o ouvinte.**

A digitalização global facilitou e acelerou o acesso de fraudadores a este modelo de golpe, o que é preocupante, pois **distinguir entre um conteúdo de deepfake e um real pode ser extremamente desafiador.**

Segundo a Onfido, empresa especialista em verificação de identidade, **o número de fraudes que utilizam a técnica de deepfake aumentou 31 vezes de 2022 para 2023,** juntamente com outras tecnologias capazes de gerar informações realistas, como imagens, textos e áudios. Aplicativo de face-swaps e o crescimento exponencial da Inteligência Artificial estão profundamente ligados com esse número.



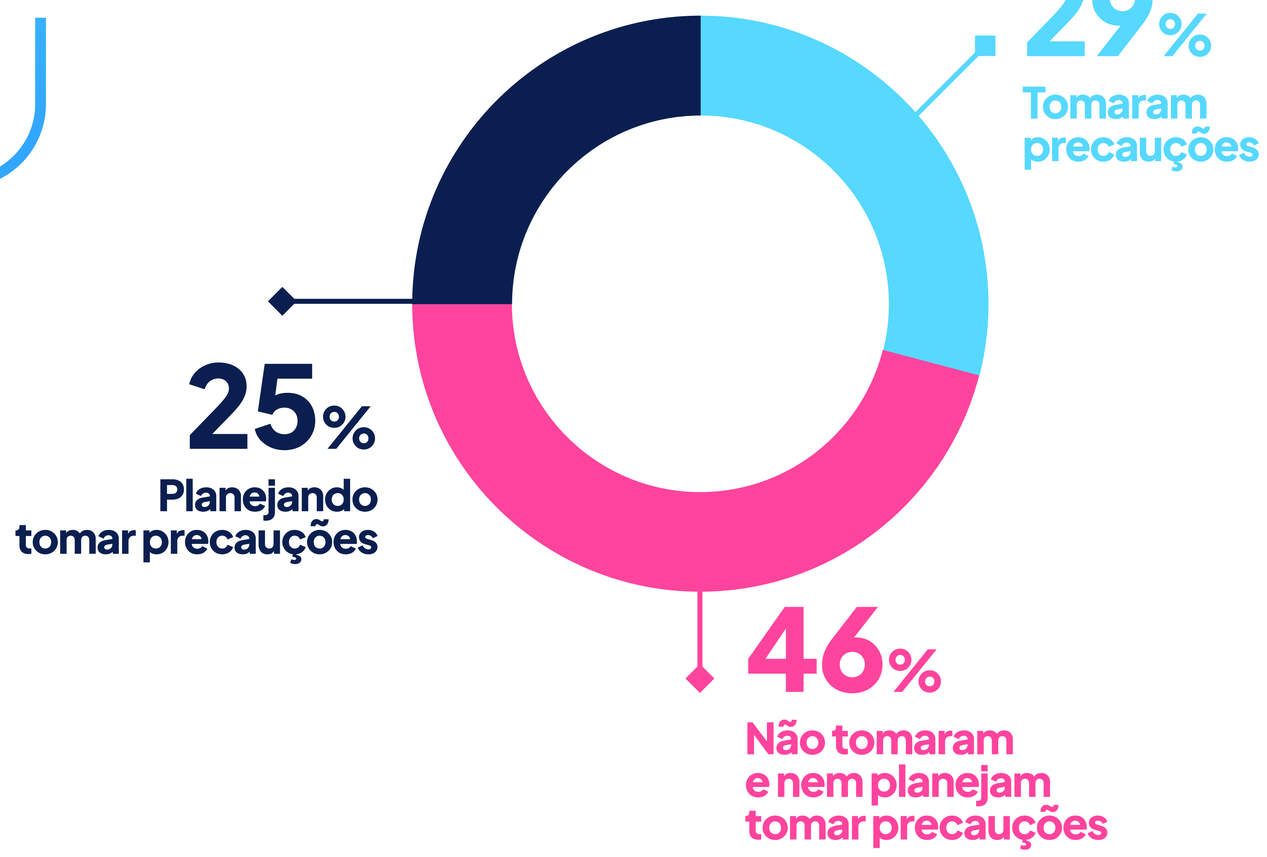
Fonte: Onfido

Além da esmagadora quantidade de deepfakes realizadas nos últimos anos, essa modalidade de fraude apresenta outra grande ameaça: Sua dificuldade de ser detectada.

O avanço tecnológico permite que diversos sistemas IA ensinem ou até mesmo produzam algum modelo de deepfake. Existem mais de **100 mil modelos de IA que podem criar deepfakes, mas menos de 3% são capazes de detectá-los.**
As empresas também não têm tomado as medidas de proteção necessárias. De acordo com a Pesquisa Inaugural de Deepfakes em Negócios, quase **50% das empresas não possuem um plano de proteção contra os ataques de deepfake.**

Fonte: Attestiv

As empresas são muito lentas para agir.



A tendência dessa fraude

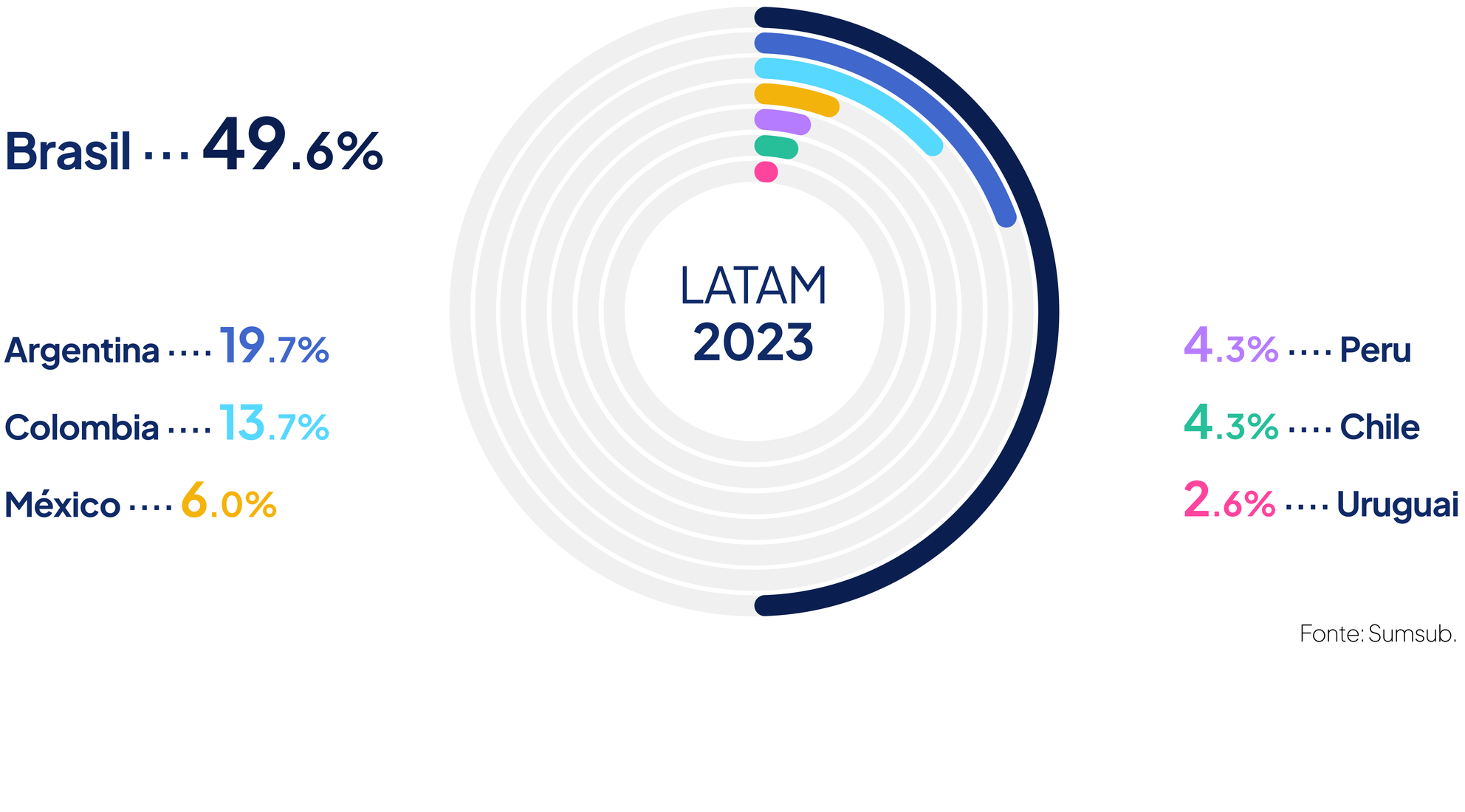
Sem dúvida, os golpes de deepfakes alteraram significativamente o panorama das fraudes atuais.

Um pequeno número de fraudadores é responsável por milhares de ataques. Um único fraudador pode submeter centenas de identidades criadas por deepfakes em pouquíssimo tempo, abrindo caminho para uma série de crimes semelhantes.

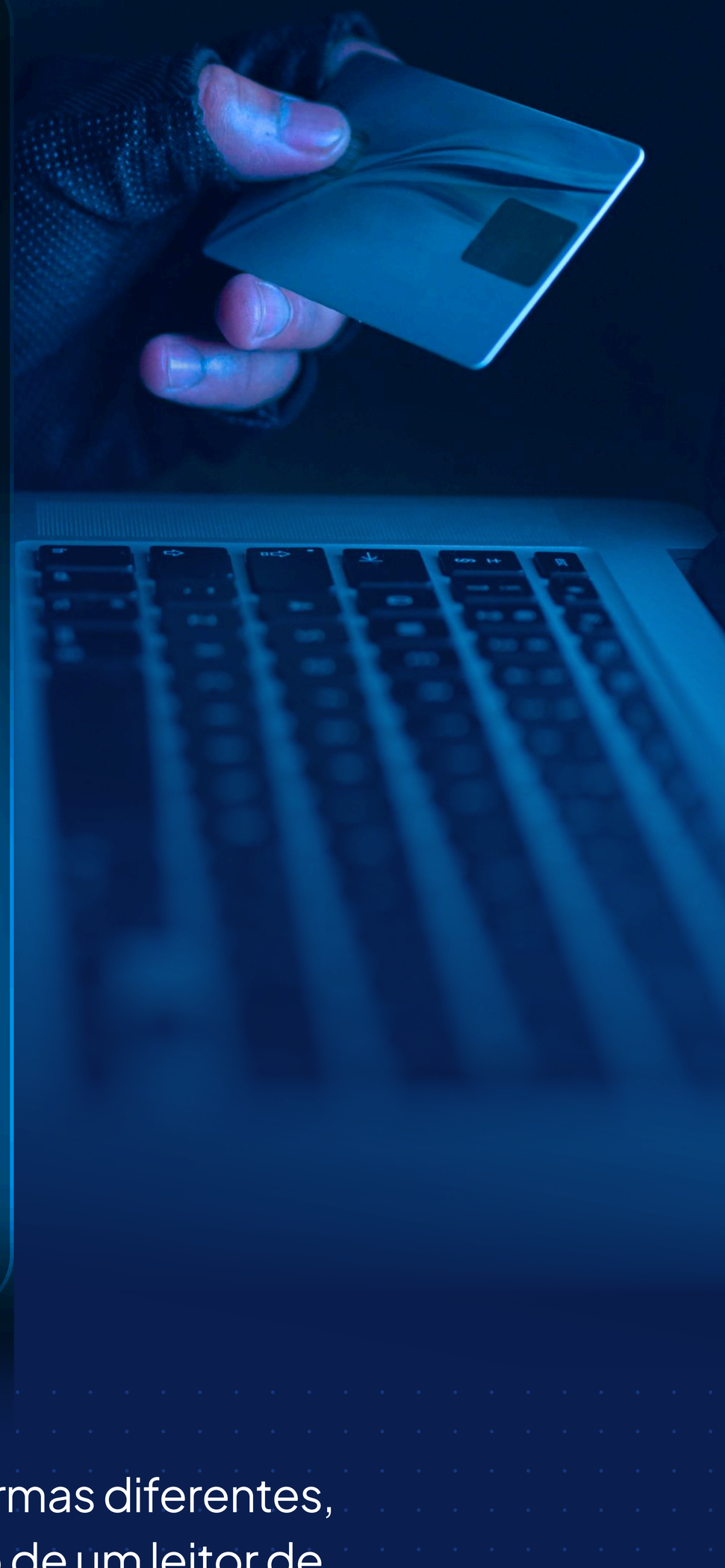
Por exemplo, em 2019, o CEO de uma empresa inglesa foi enganado por um áudio deepfake e, acreditando estar no telefone com seu chefe, fez um depósito de 220 mil euros, sem saber que estava depositando na conta de um fraudador. No ano seguinte, um golpe similar foi aplicado em um homem da China, que perdeu cerca de 35 milhões de dólares ao investir em um projeto inexistente. Esses incidentes destacam os perigos reais e as consequências financeiras devastadoras associadas aos deepfakes.

Também é comum que criminosos se concentrem em empresas específicas, piorando ainda mais as consequências do ataque por ser um planejamento fraudulento de longo prazo. Em 2023, um vídeo deepfake publicado no YouTube apresentava Elon Musk, CEO da Tesla, aplicando um golpe de criptomoeda.

Dos países da América Latina, o Brasil é o que mais apresenta casos de deepfakes, resultando em quase metade de todos os casos reportados. A taxa de crescimento para este tipo de fraude é mais de 410% de 2022 para 2023.



Fonte: Sumsub.



Fraudes em pagamentos digitais

Atualmente, os usuários têm várias opções para pagamentos digitais, como cartões, carteiras digitais, pagamentos instantâneos, internet banking, QR Code e vários outros métodos.

No entanto, **com essas inovações surgem mais oportunidades para criminosos explorarem em busca de ganhos financeiros**. Por exemplo, no Reino Unido, a fraude por aproximação aumentou 82% em 2023, o roubo de identidade de cartões aumentou 97%, e cartões perdidos e roubados geraram perdas de £100,2 milhões.

A fraude de pagamento pode assumir muitas formas diferentes, desde o roubo de números de cartão de crédito de um leitor de cartão desprotegido até e-mails falsos maliciosos. Por exemplo, uma pesquisa de 2021 da Tessian mostrou que funcionários nos EUA recebem, em média, **14 e-mails por ano que os incitam a tomar ações financeiramente fraudulentas**. Em algumas indústrias, esse número é muito maior, com trabalhadores do varejo recebendo em média 49 e-mails fraudulentos a cada ano.

Segundo a Federal Trade Commission (2024), a fraude com cartão de crédito foi o tipo mais comum de roubo de identidade no primeiro semestre de 2024, com 215.000 casos relatados.

Isso coloca os casos de fraude com cartão de crédito aproximadamente no mesmo ritmo do ano de 2023 e abaixo do número de casos relatados em 2022.

De 2017 a 2019, a fraude com cartão de crédito foi o tipo mais comum de roubo de identidade, sendo superada apenas por **fraudes com documentos e benefícios do governo** em 2020 e 2021, quando os golpistas aproveitaram os programas de benefícios governamentais da era da pandemia.

Ainda assim, houve um aumento de **49% nos casos relatados de fraude com cartão de crédito** em 2020 em comparação com 2019. Em 2023, houve **53% mais casos relatados de fraude com cartão de crédito** do que em 2019.

Além disso, um estudo da fintech Silverguard revelou que **42% dos brasileiros já foram vítimas de golpes relacionados ao Pix**. Em 2023, houve 2,5 milhões de golpes do tipo no país. A pesquisa, que envolveu 1.910 entrevistas e dados do SOS Golpe, indica que a **engenharia social é a principal tática dos golpistas**, com 70% dos casos envolvendo manipulação da vítima. Os golpes mais comuns incluem pedidos de dinheiro se passando por parentes e oportunidades de investimento falsas. A maioria dos golpes começa nas redes sociais, e as vítimas, especialmente idosos, sofrem grandes prejuízos financeiros.

A tendência dessa fraude

São muitas as formas pelas quais os fraudadores burlam os sistemas de pagamentos digitais:

1. Phishing

O phishing é um tipo de ataque de engenharia social que visa enganar as pessoas por meio de manipulação psicológica. Nesses ataques, **fraudadores utilizam e-mails, mensagens de texto ou sites falsos para obter informações sensíveis**, como credenciais de login e dados de cartões de crédito. Geralmente, esses e-mails parecem ser de fontes confiáveis, como bancos ou lojas online renomadas, e solicitam que o destinatário clique em um link para atualizar informações da conta, verificar uma transação recente ou reclamar um prêmio. **Ao clicar no link, a vítima é direcionada para um site falso onde deve inserir dados pessoais.**

O phishing pode também ocorrer via mensagens de texto (conhecidas como "smishing") ou em redes sociais ("pharming"), onde links ou mensagens falsas são usadas para obter informações pessoais ou instalar malware.

---

2. Skimming

O skimming acontece quando um fraudador utiliza um **dispositivo chamado "skimmer" para roubar informações de cartões de crédito ou débito.** O skimmer é instalado em leitores de cartões em caixas eletrônicos ou terminais de ponto de venda, como caixas de autoatendimento. Esse dispositivo captura os dados da faixa magnética do cartão, que podem ser usados para criar cartões falsos ou fazer compras fraudulentas.

Além dos skimmers, **os fraudadores também podem usar pequenas câmeras ou sobreposições para capturar o PIN do cliente**. Essas informações são então usadas com os dados roubados do cartão para realizar saques ou compras não autorizadas.

3. Roubo de identidade

O roubo de identidade ocorre quando um **fraudador rouba informações pessoais, como nome, número de CPF ou dados de cartão de crédito**, e as utiliza para realizar compras não autorizadas ou abrir contas em nome da vítima. Esse tipo de fraude pode ter graves consequências financeiras e legais, além de causar estresse significativo.

O roubo de identidade pode incluir várias táticas, como ataques de phishing, vazamentos de dados de grandes empresas, ou roubo de correspondências, bolsas ou carteiras. Uma vez que o fraudador obtém as informações pessoais, pode usá-las para **abrir contas de crédito, solicitar empréstimos ou até mesmo declarar impostos fraudulentos.**

---

4. Fraude de *chargeback*

A fraude de chargeback, ou "fraude amigável", ocorre quando um cliente **contesta uma transação legítima, alegando que não fez a compra ou que não recebeu o produto ou serviço pago**. Em alguns casos, o cliente pode receber um reembolso e ainda manter o produto ou serviço, resultando em perda financeira para o negócio. A fraude de chargeback pode resultar em perda de receita e taxas e penalidades para o negócio.

Esse tipo de fraude pode ocorrer quando um cliente faz uma compra legítima e depois contesta a cobrança com a empresa de cartão de crédito, ou quando um cliente usa intencionalmente um cartão roubado e depois contesta a transação como não autorizada.

---

4. Comprometimento de e-mail corporativo

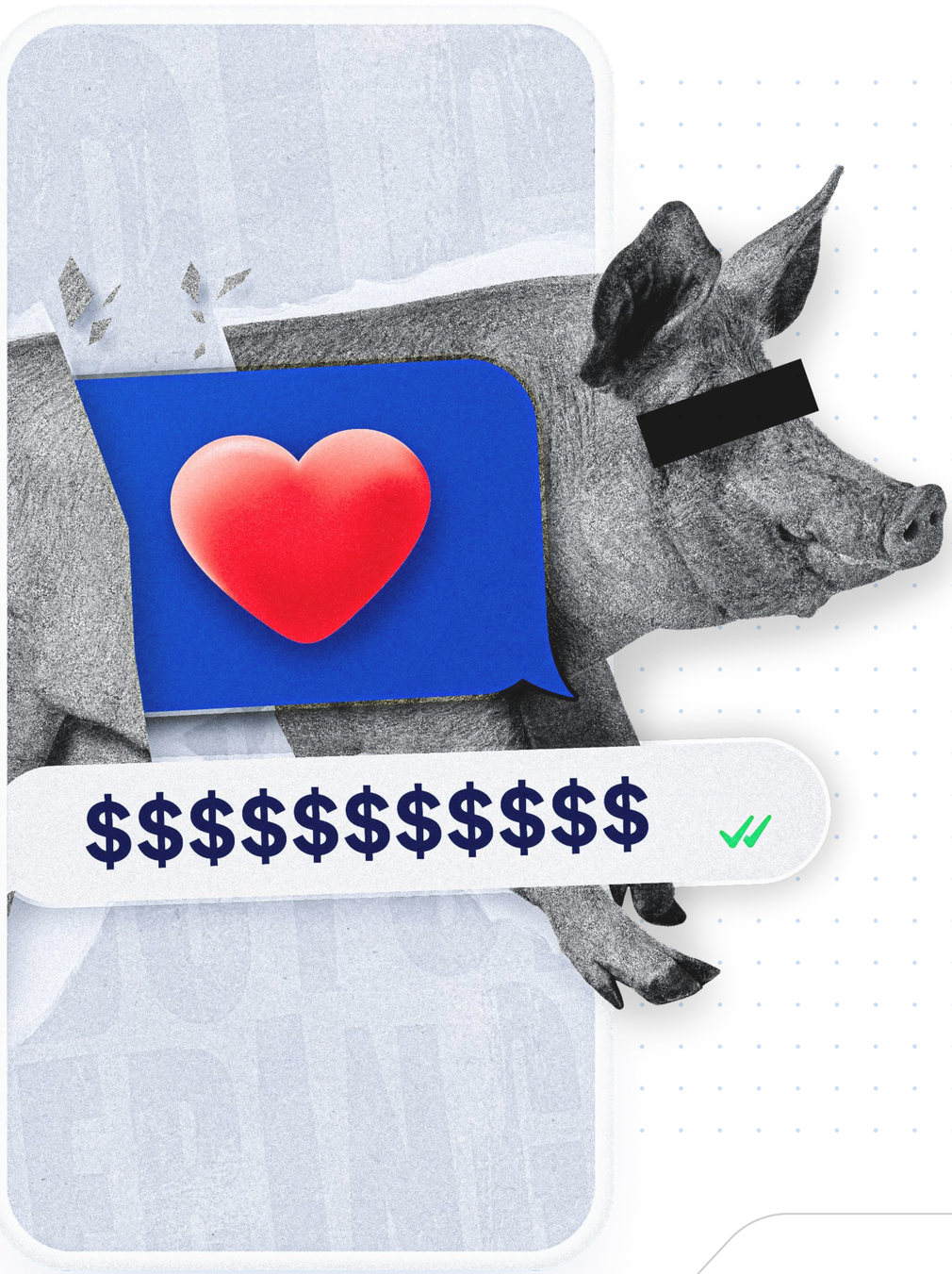
O comprometimento de e-mail corporativo é um tipo de fraude onde e-mails enganam funcionários para que transfiram dinheiro para contas fraudulentas. Os fraudadores **geralmente acessam uma conta de e-mail corporativo através de phishing ou táticas de engenharia social e enviam e-mails solicitando transferências de dinheiro.**

Esses e-mails podem se passar por executivos de alto nível ou fornecedores, solicitando pagamentos urgentes. O e-mail pode parecer legítimo, utilizando a marca da empresa e um endereço de e-mail familiar. Se o funcionário seguir as instruções, o dinheiro será transferido para a conta dos fraudadores.

---

6. *Pig Butchering*

"Pig Butchering" é um termo usado para descrever um tipo de fraude financeira que envolve **enganar vítimas para que elas invistam grandes quantias de dinheiro em esquemas fraudulentos**. O nome vem da analogia com o processo de engorda de um porco antes do abate, simbolizando o processo de enganar a vítima para extrair o máximo de dinheiro possível antes de "abater" ou desaparecer com os fundos.



De acordo com a edição de 2024 do Relatório de Ameaças Bianual da Visa, os golpes de "pig butchering" emergiram como uma das quatro principais ameaças de pagamento contra os consumidores. Nesses esquemas, os fraudadores procuram vítimas em sites de namoro e redes sociais e criam contas falsas para interagir com elas. O objetivo é ganhar a confiança da vítima e se tornar seu "amante" ou "amigo". O golpista pode até fingir ser um contato há muito perdido da vítima.

Em 2023, o Federal Bureau of Investigation (FBI) **registrou mais de US$3,5 bilhões em perdas relatadas em relação ao "pig butchering"**, correspondendo a cerca de **40.000 vítimas**. À medida que GenAI e outras tecnologias emergentes se desenvolvem, golpes como o "pig butchering" se tornarão cada vez mais convincentes, "levando a perdas sem precedentes para os consumidores", de acordo com o diretor de risco e serviços ao cliente da Visa.

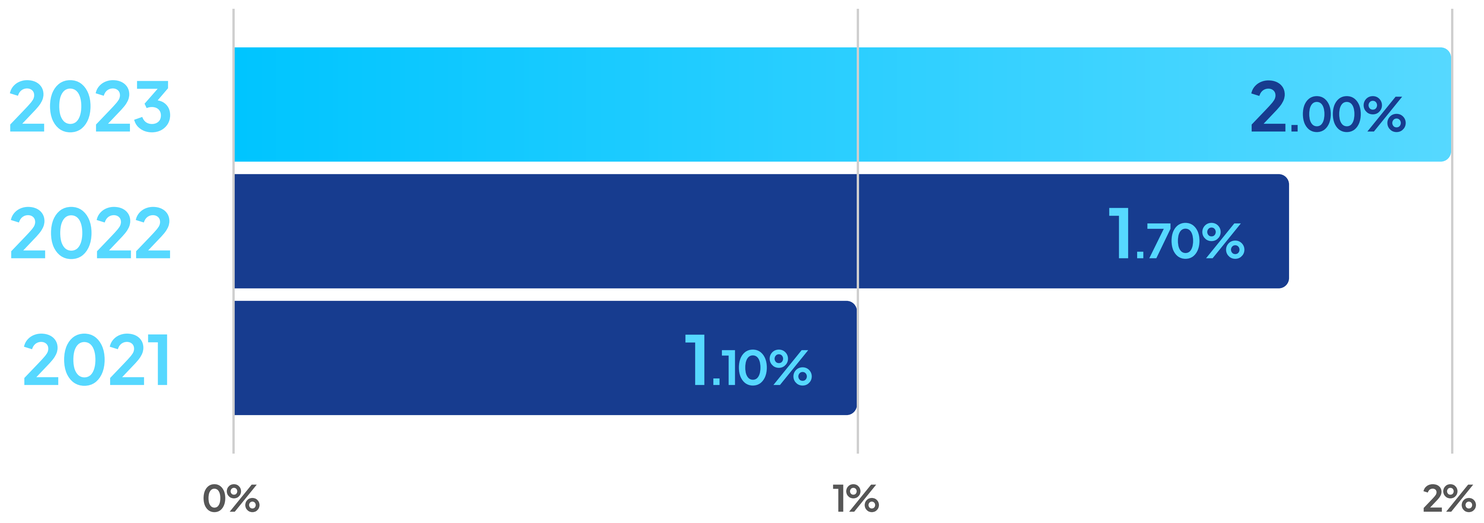
Identidades falsas

A digitalização também promoveu um aumento nos ataques direcionados a documentos de identidade e, mais especificamente, como fraudá-los. O avanço tecnológico permite o acesso a ferramentas mais sofisticadas que facilitam o trabalho dos fraudadores.

A ameaça desse tipo de fraude é ampliada ao considerarmos as diversas portas que uma identidade falsa pode abrir. Os fraudadores podem utilizar da identidade roubada para uma variedade de motivos, como a **veiculação de documentos falsos, a abertura de contas de crédito, obtenção de empréstimos e realização de compras.**

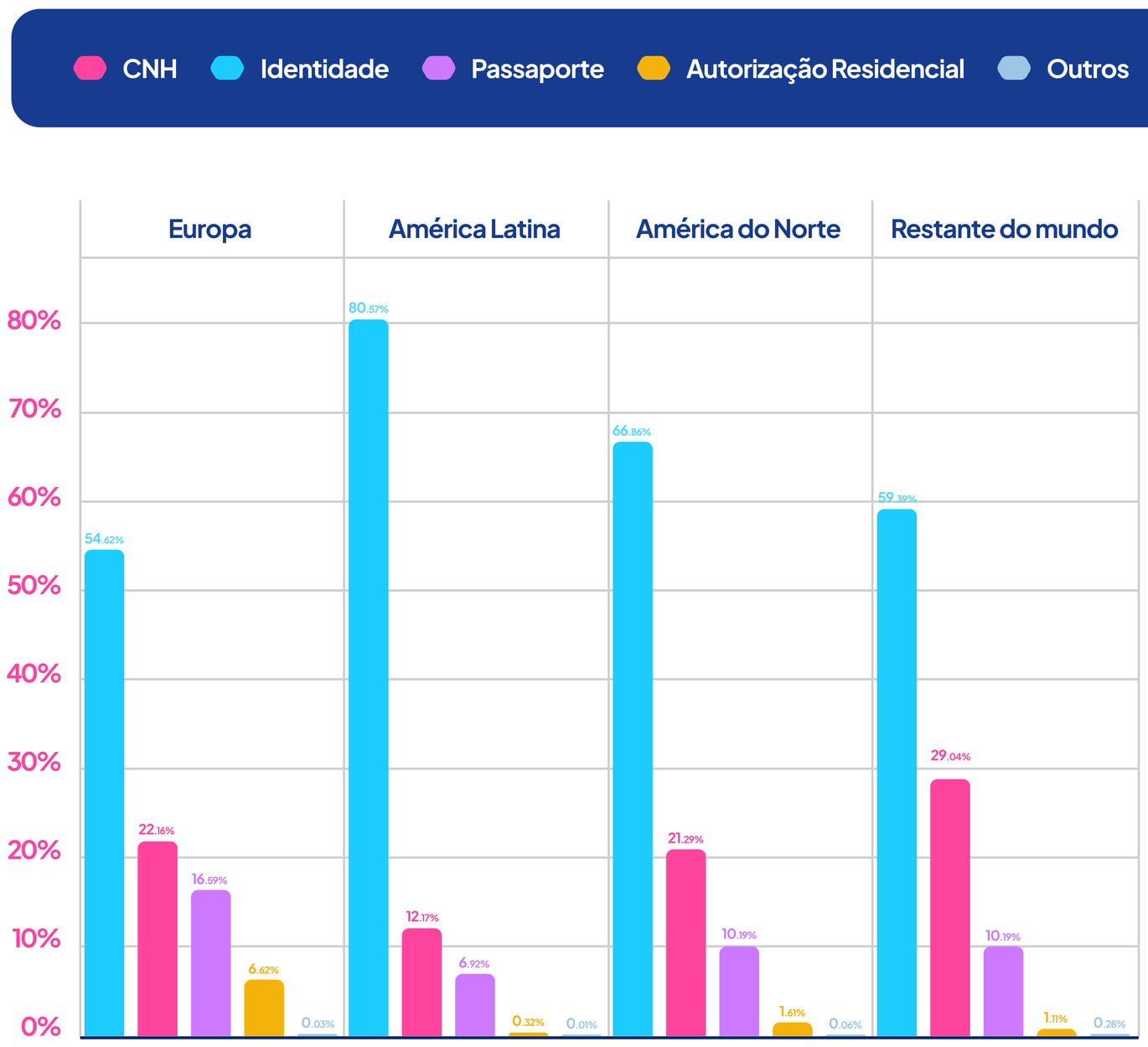
Esse tipo de fraude é um dos mais complexos ataques dos últimos anos, já que pode ser realizado de formas variadas e com documentos diferentes. Alterando fotos, informações e fontes, fraudadores podem realizar a fraude física ou digitalmente. Apesar da fraude física ser mais comum, **a fraude no meio digital teve um crescimento de 18% no ano passado.**

Assim como as fraudes de deepfake, a fraude em documentos no meio digital **tende a crescer devido ao avanço da inteligência artificial e a facilidade e praticidade oferecida pelas plataformas digitais**. A quantidade de fraudes de identidade teve seu número praticamente dobrado desde 2021 e, em 2022, 57% dos consumidores ou conheciam alguém ou foram eles próprios vítimas de fraudes de identidade.



Fonte: Sumsub.

Documentos de identidade foram os mais forjados ao redor do mundo em 2023, sendo quase **47% dos documentos de identificação a sofrerem este tipo de ataques**. **A CNH brasileira é o documento menos forjado do mundo,** mas isso não protege o país desses ataques de fraude.



Fonte: Veriff

O receio desse tipo de golpe é evidente nos dados, que mostram que **92% dos consumidores do Brasil já deixaram de comprar online por achar que a loja se tratava de fraude**, enquanto que **42% dos respondentes já foram vítimas de golpe durante alguma transação online**.

A tendência dessa fraude

Quando falamos da fabricação de identidades falsas, a principal tendência pode ser resumida na ameaça das fraudes biométricas. Elas consistem em criminosos se passando por outras pessoas – as vítimas do ataque, no caso.

Os cibercriminosos empregam dois métodos principais na hora de realizar as fraudes biométricas. Para tentar fraudar a identidade de alguém, eles podem capturar a foto de uma tela com o rosto de outra pessoa. Essa foto pode ser a foto de algum perfil de uma rede social ou até mesmo de um banco de imagens. Outro método é a **utilização de uma foto de um documento na tentativa de burlar o sistema para não usar um rosto de verdade.**

As técnicas de fraude podem ser divididas em três tipos diferentes: **Selfies, vídeos e motion.** Dentro de cada um desses modelos, existem estratégias que podem ser utilizadas para a realização da fraude biométrica, mas as mais comuns são fotos e vídeos exibidos na tela.

Essas fotos e vídeos apontam para procedimentos de deepfake, mostrando novamente a ligação entre esses dois tipos de fraude que utilizam ferramentas digitais para editar o rosto de alguém durante a captura de uma tela. Além disso, outras técnicas utilizadas por fraudadores são:

- **Spoof ID: Foto da imagem de um documento de identificação;**
- **Spoof impresso: Foto de uma imagem impressa;**
- **Máscara 2D;**
- **Máscara 3D.**

Fonte: Onfido

Invasão de contas bancárias

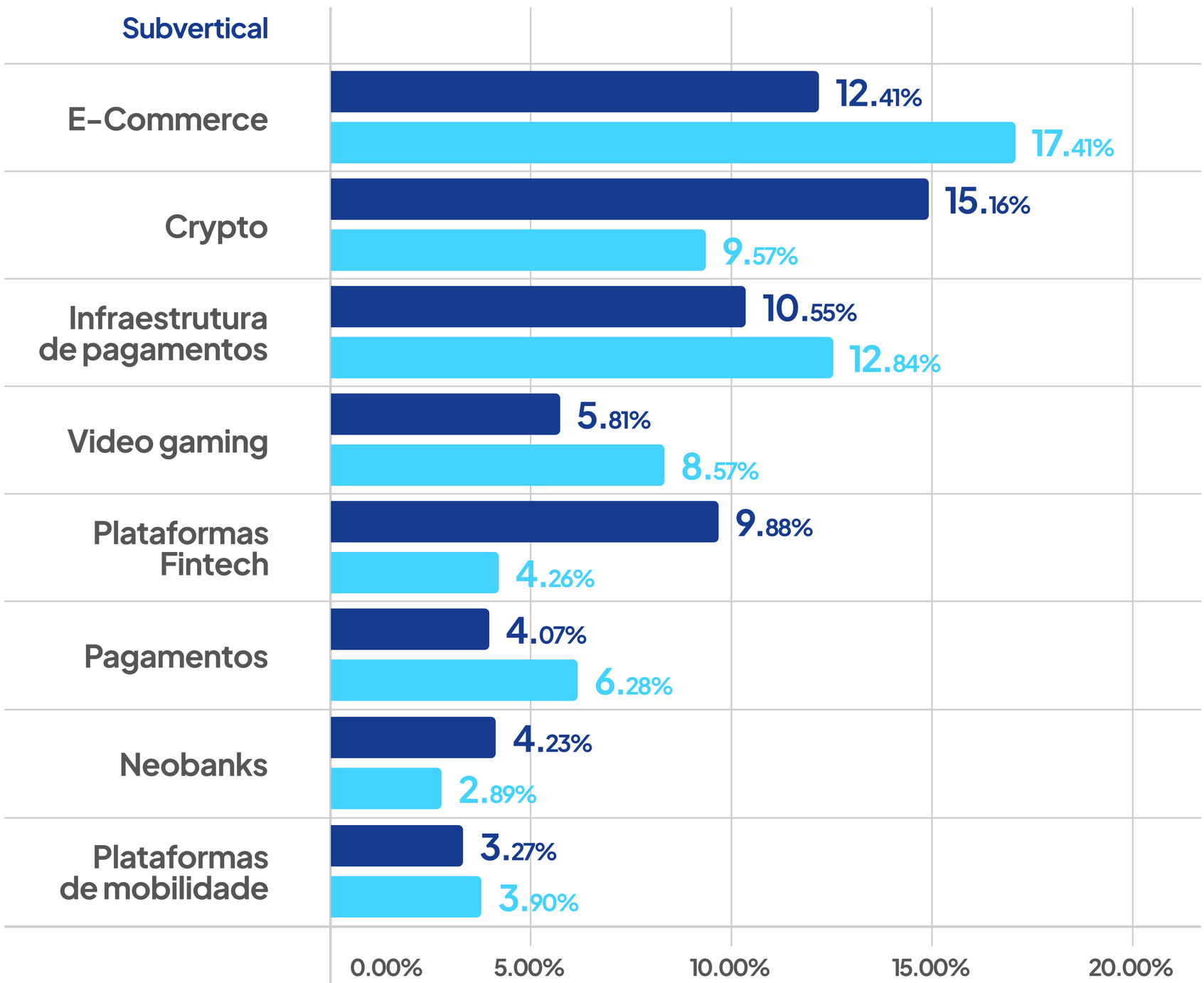
As fraudes por invasões de contas bancárias acontecem quando um fraudador consegue acesso às informações de login da vítima, utilizando-as para roubar patrimônio ou dados sobre a mesma. Apesar desse modelo de fraude trazer características de fraudes de identidade, as invasões de contas bancárias são consideradas **fraudes creditícias, uma vez que o processo precisa de informações sensíveis para ocorrer.**

Existem diversas contas que um fraudador pode invadir, como contas bancárias, cartão de crédito e plataformas de e-commerce. Uma vez dentro dessas contas, os dados da vítima são considerados tão valiosos quanto o dinheiro encontrado. Informações como e-mail, senhas e números de cartão de crédito podem levar a transações falsas, fraudes no cartão de crédito e compras não autorizadas pelo consumidor.

Após conseguir o acesso, a maioria dos criminosos irá tentar evitar qualquer atividade suspeita que possa comprometer sua invasão. Para isso, eles mudam as informações identificáveis da vítima e suas senhas, além de adicionarem um novo usuário e pedirem um novo cartão.

Com todas essas medidas, os cibercriminosos podem realizar transações que parecem legítimas, além de terem a possibilidade de vender a conta ou os dados da vítima para terceiros.

Comparação da taxa média anual de fraude para setores verticais 2022 x 2023



Fonte: Veriff

A tendência dessa fraude

Os ataques usando esse tipo de fraude aumentam conforme os métodos usados pelos fraudadores se desenvolvem. Destacamos algumas formas mais comuns que os cibercriminosos podem usar para tentar invadir alguma conta:

1. Preenchimento de credenciais

É muito comum que fraudadores comprem na Dark Web uma lista de credenciais roubadas. Essas listas contêm dados como endereços de e-mail e suas senhas correspondentes, e normalmente são formadas a partir de bots automatizados para tentar acessar certas contas. Uma vez captada, essa informação pode ser **utilizada para acessar outras contas da vítima, partindo do princípio que muitas pessoas tendem a reutilizar senhas e nomes de usuário.**

---

2. Troca de chip

Quando um cliente compra um novo celular que não é compatível com seu antigo chip, este chip é substituído por um novo. Esse é um serviço legalizado e realizado por diversas empresas, mas os fraudadores **podem utilizar desse processo e transferir o número de telefone da vítima para um novo chip**. Com esse método, os aplicativos bancários da vítima podem ser acessados e manipulados pelo golpista, uma vez que a autenticação do aplicativo pode ser feita via SMS.

3. Malware

Malware são softwares programados intencionalmente para causar danos, e são outra maneira que cibercriminosos podem acessar os aparelhos eletrônicos de alguém. Ao fazer o download de um aplicativo por meio de uma fonte suspeita, a **vítima pode ter seus dispositivos interceptados e seus dados roubados.**

4. Cavalos de Tróia

Quando falamos de aplicativos de bancos, um método de invasão comum são os cavalos de Tróia. Nesse método, **uma tela falsa é posta em cima de uma aplicação de banco legítima.** Assim, um malware pode ser instalado e continuar no dispositivo enquanto a vítima realiza suas transações bancárias.

5. *Phishing*

Phishing, que faz alusão a pescar (*fishing*, em inglês), é o método de **invasão de contas bancárias mais utilizado por fraudadores**, e por essa razão, possui uma tendência maior de crescimento. Essa técnica de fraude consiste, basicamente, em fraudadores fingirem ser marcas ou indivíduos.

Ao personificar uma empresa, **os golpistas podem usar de técnicas de manipulação para convencer as vítimas a clicarem em links que as direcionam para páginas com malwares instalados para roubar seus dados**. Na maior parte das vezes esse contato é feito através de um email, mas também pode ser feito por SMS ou até mesmo através de redes sociais.

A maneira como a maior parte das pessoas utiliza e protege suas informações também está relacionada com o golpe. O uso constante de aparelhos na vida cotidiana aumenta a possibilidade de tentativas. Por exemplo, em 2022, um estudo da Proofpoint apontou que **78% dos entrevistados usavam dispositivos de trabalho para atividades pessoais, e 72% utilizava dispositivos pessoais para atividades de trabalho.**

Com essa mesclagem de atividades e alta frequência de uso, a abertura para golpes de phishing aumenta, sendo evidenciado também pelo fato de que **apenas 37% dos entrevistados sabia que links de empresas podem levar para páginas que não da mesma.**

Sabem que arquivos salvos na nuvem nem sempre são seguros.

Sabem que e-mails internos do trabalho nem sempre são seguros.

Sabem que um link no e-mail podem não corresponder ao site que aparenta.

Sabem que a empresa em que trabalham não podem automaticamente bloquear todos os e-mails maliciosos.

Usam equipamentos do trabalho para atividades pessoais.

Usam equipamentos pessoais para atividades relacionadas ao trabalho.

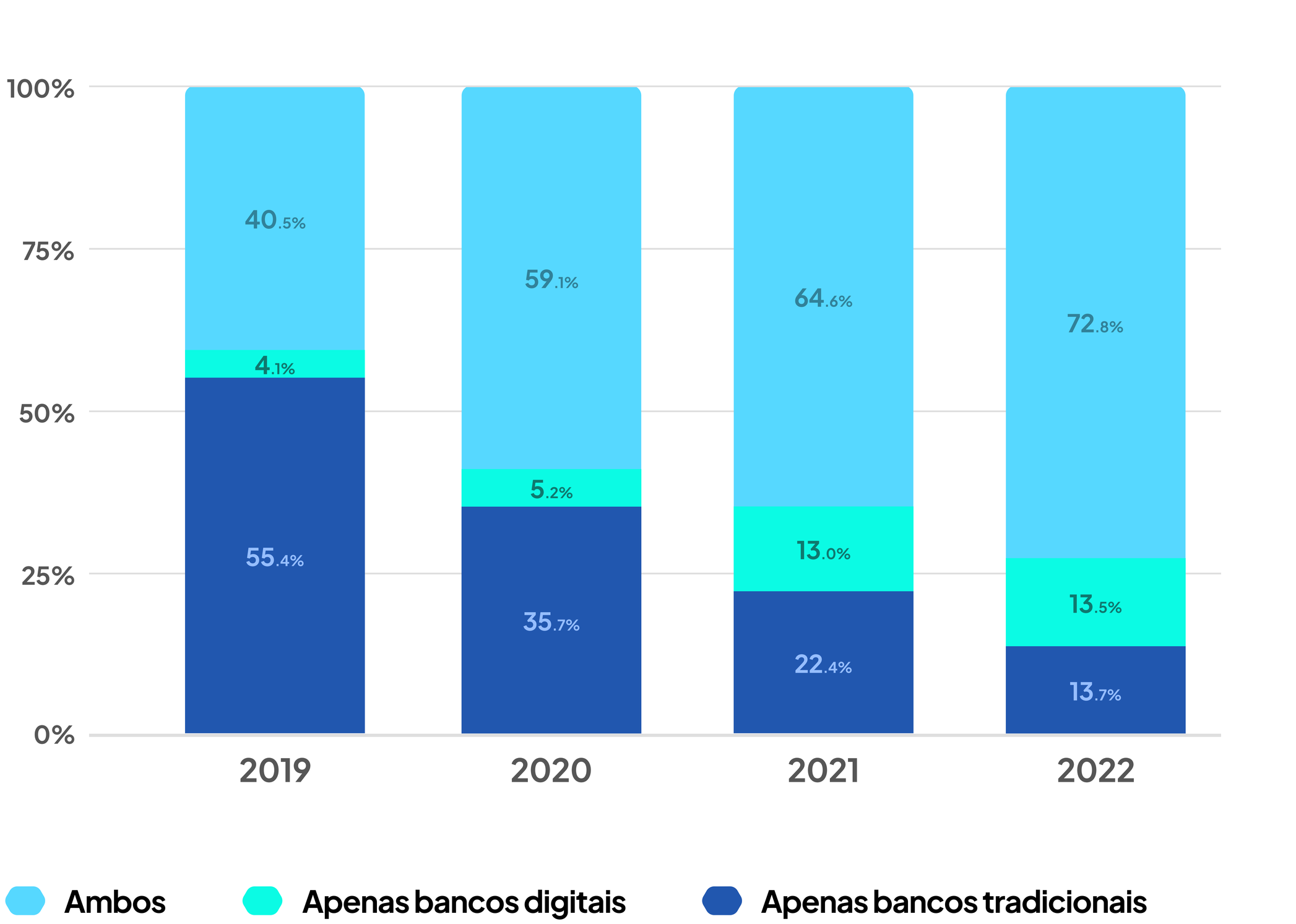
Deixam amigos e familiares usarem seus equipamentos de trabalho.

Fonte: Proofpoint

Soluções de mitigação de fraude da QI Tech

Dado todos os riscos apresentados neste material, é essencial que as empresas incorporem uma camada de segurança em todos os seus serviços e produtos. O desenvolvimento de soluções antifraude no mercado dialoga diretamente com o crescimento tecnológico encontrado na maioria das empresas atuais. Essas soluções são essenciais para proteger não apenas os próprios negócios, mas também os dados e a privacidade dos clientes, garantindo assim a confiança e a integridade das operações comerciais.

O uso de novas tecnologias em serviços empresariais é traduzida pelo comportamento do consumidor atual, que utiliza a digitalização na maior parte de seu cotidiano. Por exemplo, de **2019 a 2022, o número de clientes que faziam uso apenas de bancos digitais cresceu de 4,1% para 13,5%.**



Fonte: Math Group

Um estudo sobre o comportamento de e-commerce também apontou que o que influencia os compradores brasileiros na hora de fechar uma compra online é a facilidade de compra, aspecto chave da digitalização que passa a participar das mais variadas empresas.

Em 2023, um estudo realizado pela Digibee, solução de integração low-code para empresas, apontou que, das mais de mil empresas entrevistadas**, 71% delas estavam planejando adotar, complementar ou substituir sua tecnologia de integração**, mostrando a necessidade destas de se adaptarem a um contexto digital baseado na agilidade de processo.

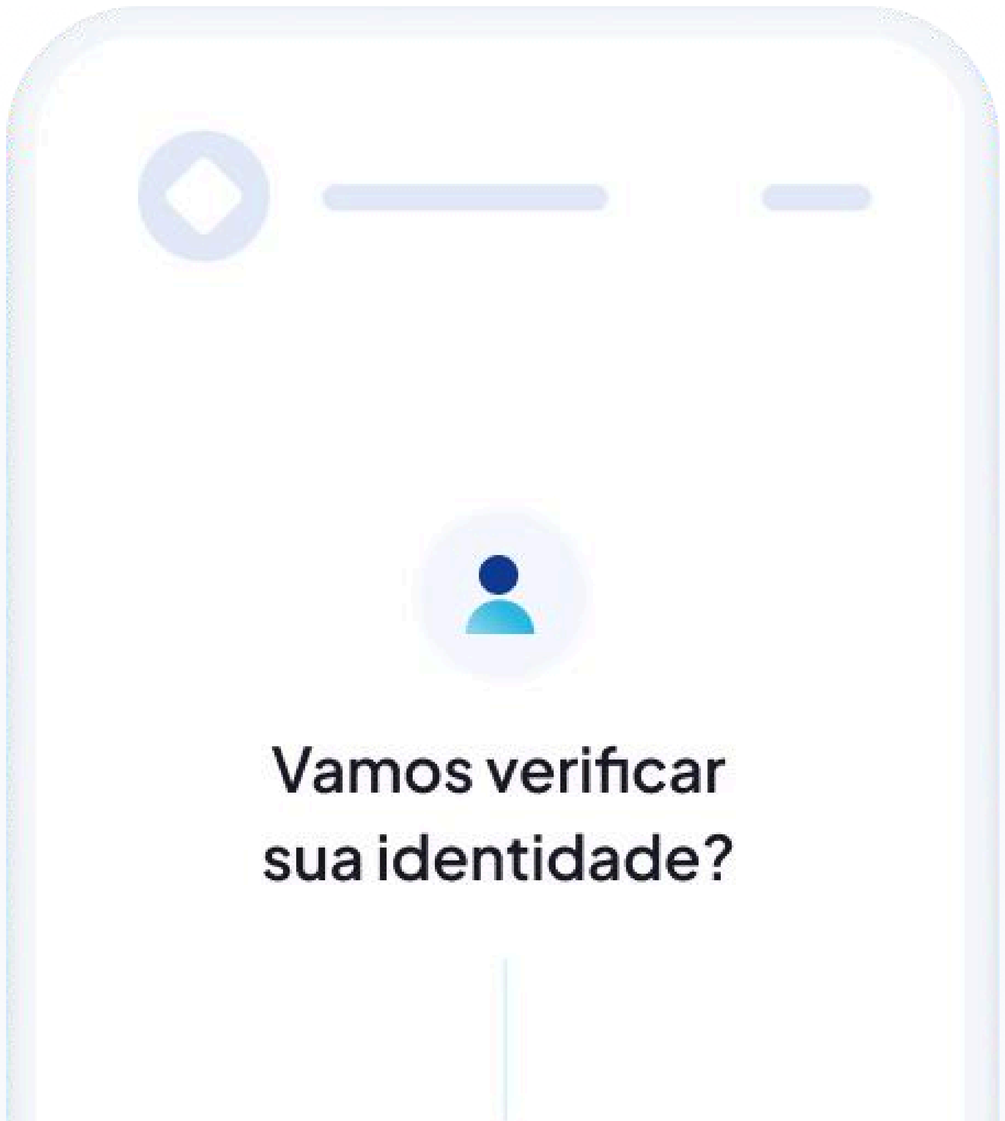
Por outro lado, a agilidade pede por proteção, o que se reflete no dado de que **33% das empresas afirmaram que um dos maiores desafios de implementar um novo sistema de integração é a questão da segurança.**

Sendo assim, faz-se necessária a utilização de soluções que mitiguem fraudes.

> **“Na QI Tech, possuímos uma série de produtos e serviços de fácil integração que apoiam empresas a diminuírem os riscos de fraudes de ponta a ponta”.**
>
> Ricardo Alfaro – Sócio da QI Tech

Onboarding

Para manter as operações e produtividade da empresa, **é preciso que as companhias conheçam seus clientes de uma forma segura e eficiente**, e é nessa necessidade que o onboarding se encaixa. Dividido em diversas soluções, essa operação é responsável por toda a validação de usuários.



Validação cadastral

A validação cadastral é um **processo que assegura a integridade e a conformidade dos clientes**, sejam eles pessoas físicas ou jurídicas. Este processo é fundamental para garantir a segurança e a legalidade nas operações financeiras e comerciais.

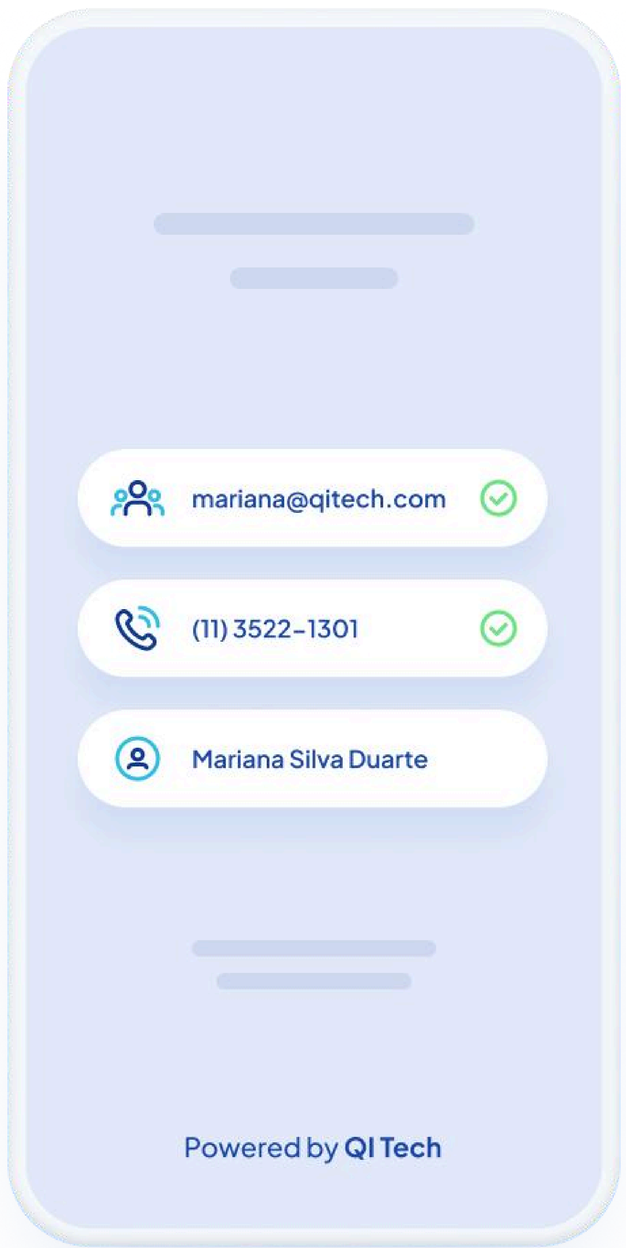
A QI Tech oferece um serviço de verificação rápida que permite identificar quem é o usuário em poucos segundos, o **background check.** A partir desse processo, os documentos dos clientes são avaliados com uma verificação completa, que vai desde dados básicos até uma análise mais aprofundada. A operação de background check também identifica usuários suspeitos, uma vez que a **QI Tech** utiliza informações de instituições respeitadas, como o FBI, para identificar e barrar perfis de risco, como endereços suspeitos e históricos criminais.

A integridade do sistema da empresa depende também da conformidade regulatória. A **validação de compliance** é responsável por toda a averiguação das diretrizes legais empresariais que, além de serem essenciais para sua operação, são obrigatórias para o desenvolvimento tecnológico da mesma.

Análise de documentos

A tecnologia usada por trás da análise completa de documentos é a **OCR (Optical Character Recognition), sigla para Reconhecimento Óptico de Caracteres**. Basicamente, essa tecnologia analisa as imagens e identifica os caracteres, convertendo os dados para um formato que possa ser lido e pesquisado por softwares de texto. No caso da análise de onboarding, a **OCR irá analisar os documentos pessoais que o usuário apresentar.**

Num geral, existem dois documentos que podem ser analisados: O RG e a CNH. Como foi apresentado anteriormente, a CNH é o documento de identidade menos forjado do mundo, e isso se dá pelo fato do documento seguir um padrão único em todo o país.



> **A eficiência deste processo está diretamente relacionada com a base de faces da QI Tech, que possui mais de 120 milhões de rostos. Naturalmente, quanto mais possibilidades de comparação entre usuários e os documentos apresentados, mais precisa será a análise”.** Ricardo Alfaro – Sócio da QI Tech

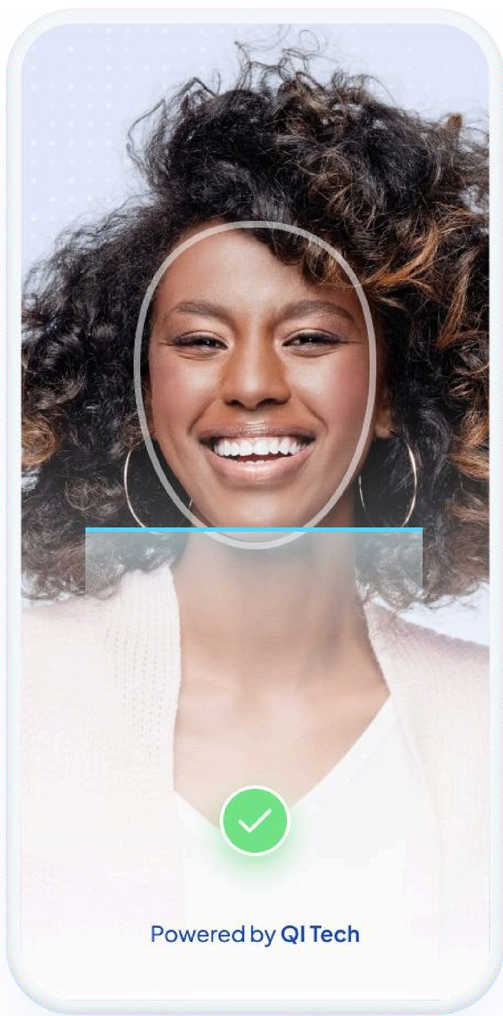
A base de faces é um banco de fotos de várias pessoas que estão vinculadas aos seus respectivos CPFs. Sendo assim, a comparação com a selfie e o documento de um potencial usuário pode ser realizada. As imagens presentes na base garantem se há alguma correspondência ou divergência com a foto tirada para a verificação, dizendo se o cliente é realmente quem ele diz ser, ou se está tentando se passar por outra pessoa.

Reconhecimento facial

O reconhecimento facial funciona a partir de sistemas de inteligência artificial, que são responsáveis pelo cruzamento de dados e detecção de padrões que garantem que o rosto detectado é de certa pessoa. **O processo de reconhecimento facial da QI Tech pode ser dividido em 3 principais etapas:**

Captação

Antes de tudo, é preciso saber que o rosto apresentado é, de fato, um rosto. A etapa de captação é responsável por detectar um rosto em uma imagem e coletar os dados faciais do cliente. Esses dados podem ser obtidos de diferentes maneiras, como imagens comuns, vídeos, gravações de câmeras de segurança e dados tridimensionais. Dentro da captação realizada pela QI Tech, é usada outra tecnologia: **Liveness.**



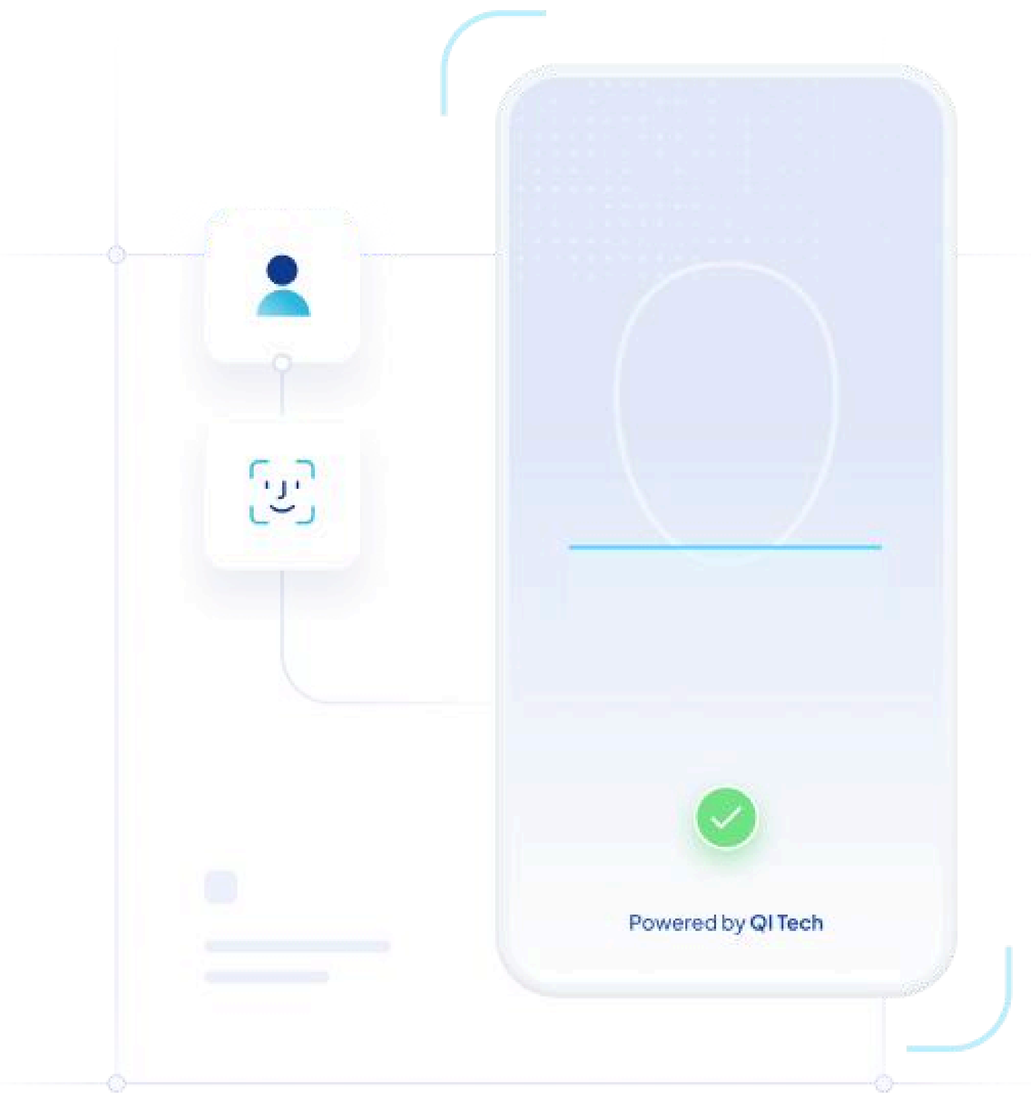
O Liveness atua como uma Prova de Vida, permitindo a distinção de uma pessoa tirando uma foto ou uma que está usando uma máscara, por exemplo. A prova de vida é uma evolução da biometria facial. Utilizando algoritmos avançados, ela analisa os dados coletados por sensores biométricos para determinar se a fonte está viva ou se é apenas uma reprodução (como uma foto de uma foto).

Este recurso é crucial para prevenir fraudes de identidade, permitindo verificar se a pessoa está realmente realizando um determinado processo pelo celular naquele momento, ou se está usando uma imagem estática na tentativa de cometer fraude. O Liveness da QI Tech utiliza da prova de vida ativa que, diferentemente da passiva, que não requer movimentos do usuário, exige que o usuário se posicione em frente à câmera e realize algum movimento, como sorrir, piscar ou levantar as sobrancelhas.

Assim, os sensores biométricos registram essas ações e, por meio de algoritmos, analisam os dados coletados em comparação com as informações e documentações fornecidas. Dessa forma, é possível evitar que fraudadores passem pelo processo usando uma foto de outra pessoa obtida ilegalmente.

Análise

A análise do rosto registrado é feita por uma tecnologia conhecida como **biometria facial,** que analisa aspectos físicos e comportamentais do usuário. O processo da biometria facial analisa e codifica os dados biométricos do usuário, que são únicos para cada pessoa, configurando características como a distância entre o nariz e os olhos, o formato da boca e o tamanho do nariz como uma assinatura facial. Após a identificação desses pontos, a imagem do usuário é capturada, codificada em uma sequência numérica e armazenada em um banco de dados.



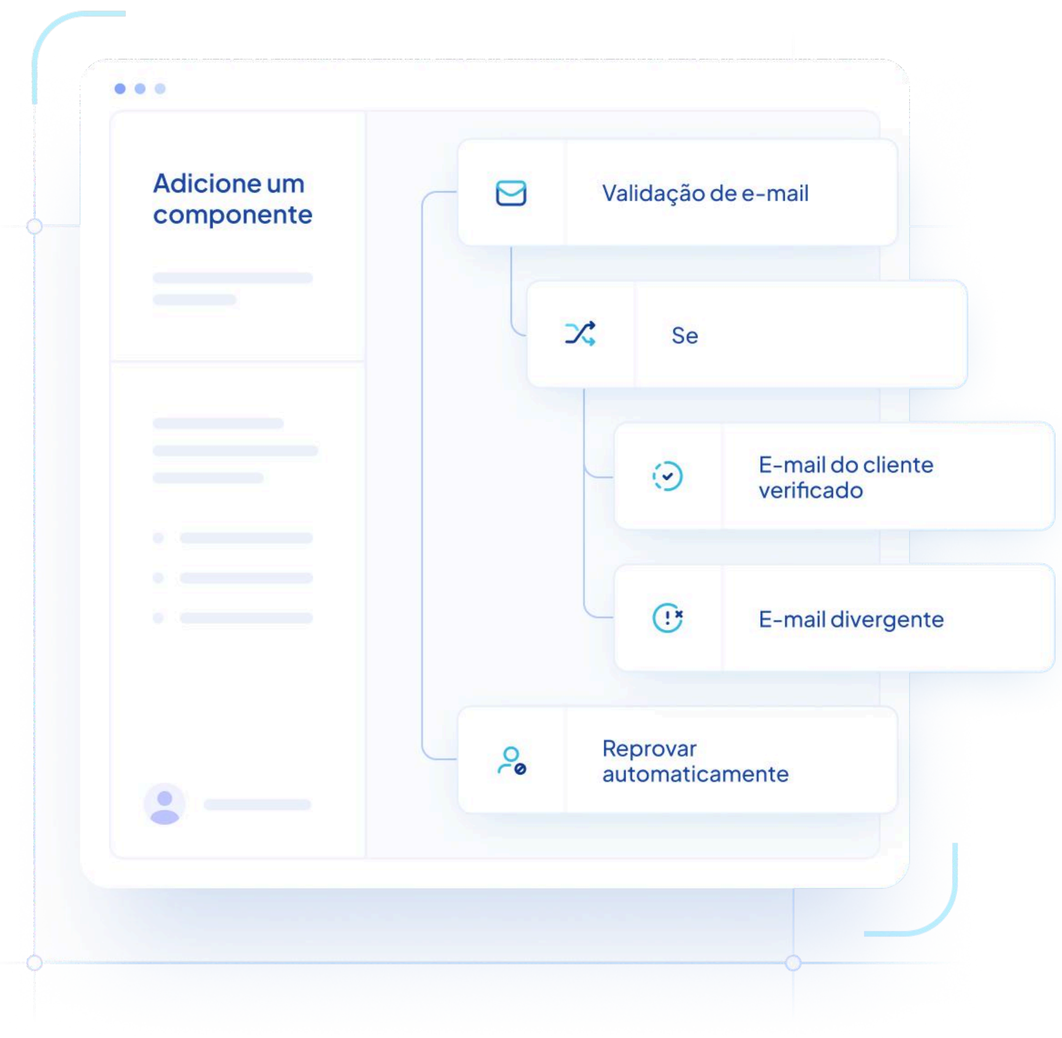
Reconhecimento

A ferramenta então analisa as imagens, comparando-as com a base de faces, utilizando técnicas de biometria facial, liveness e anti-spoofing. Esses elementos trabalham juntos para criar um perfil único e seguro para cada indivíduo, que é armazenado na base de dados. Dessa forma, quanto mais rostos houver na base, mais preciso será o reconhecimento. Ao final do processo, a validação facial confirma se o usuário é quem ele diz ser.
Além disso, a base de faces permite que o perfil seja acessado e consultado sempre que o cliente realizar uma operação financeira de maior valor ou solicitar uma alteração de dados cadastrais sensíveis, por exemplo.

Device Scan

Além do rosto e dos documentos, o dispositivo de um usuário diz muito sobre ele e a pessoa que ele apresenta ser. O **device scan da QI Tech** é uma solução que analisa o aparelho do usuário sem acessar as suas informações pessoais. Ao invés disso, a tecnologia procura por qualquer aplicativo suspeito ou dispositivos que já foram violados ou utilizados em golpes. Ademais, a geolocalização é outra parte dessa solução, responsável por analisar qualquer lugar suspeito em que o aparelho possa estar.

Motor de regras



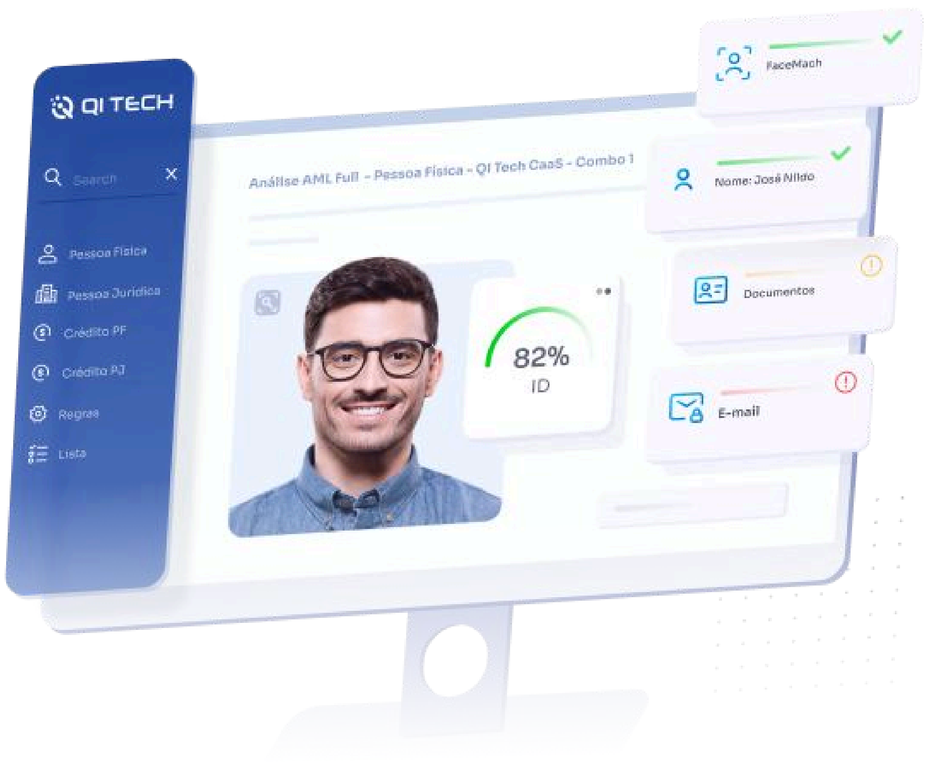
O **motor de regras** opera com uma série de critérios pré-definidos pela empresa ou sugeridos por terceiros, como especialistas ou autoridades regulatórias. Ele examina os inputs - as regras - que podem ser personalizadas de acordo com as necessidades da empresa e aplicadas em várias situações.

Fatores como cadastro e solicitações de crédito podem ser selecionados pela empresa para serem avaliados pela **QI Tech,** e a companhia também fornece uma decisão ou recomendação, como aprovação, reprovação ou encaminhamento para análise manual a partir das informações monitoradas. Ao selecionar seus próprios critérios de decisão, a empresa pode desenvolver e atualizar facilmente o mecanismo de regras conforme necessário, aumentando a autonomia e agilizando o processo.

Esse mecanismo pode ser integrado a outros sistemas e aplicativos utilizados pela empresa, como CRM, ERP e sistemas de marketing, permitindo uma automação completa e integrada dos processos. Além dos benefícios já mencionados, como automação de processos, precisão na tomada de decisões, flexibilidade e escalabilidade, essa implementação pode também melhorar significativamente a gestão de recursos e reduzir os custos operacionais.

Análise de crédito

Diferente do processo de onboarding, que se concentra em confirmar a autenticidade do usuário, o **motor de crédito na QI Tech** foca em analisar a saúde financeira do usuário. Aqui, o objetivo é validar informações relacionadas ao histórico e comportamento financeiro do usuário que podem afetar a empresa.



Por exemplo, o score de crédito é uma medida que reflete a probabilidade de um indivíduo pagar suas dívidas em dia. Ele é calculado com base em diversos fatores, como histórico de pagamentos, a razão entre crédito utilizado e o total disponível, a duração do histórico de crédito e novas solicitações de crédito. Um score alto indica um bom histórico de crédito, enquanto um score baixo pode sinalizar riscos potenciais para a companhia.

O motor de crédito também verifica todas as dívidas atuais do indivíduo. Isso inclui empréstimos, financiamentos, cartões de crédito e outras formas de crédito. Ao analisar as dívidas existentes, é possível determinar a capacidade do indivíduo de assumir novas obrigações financeiras sem comprometer sua estabilidade financeira.

Outro ponto analisado pela tecnologia são os limites de crédito, o que envolve verificar o total de crédito disponível para o indivíduo em relação ao crédito já utilizado. Isso ajuda a entender a margem de crédito disponível e a capacidade de o indivíduo contrair novas dívidas sem ultrapassar seus limites.

A forma como essa análise será feita parte completamente do cliente, que pode, utilizando o seu motor de regras, personalizar quais aspectos financeiros serão avaliados, baseado na sua operação. Ao avaliar criteriosamente os aspectos desejados, as empresas podem tomar decisões mais informadas sobre a concessão de crédito, estabelecendo condições apropriadas e minimizando riscos.

Antifraude Transacional

Bancos e contas digitais são instituições propensas a sofrerem algum ataque de fraude, e o momento de transação é uma etapa vulnerável que os fraudadores podem ter como alvo na hora de aplicarem o golpe. Entre 2021 e 2022, as **tentativas de transações fraudulentas aumentaram 92%, enquanto os valores associados a essas tentativas dispararam 146%.**

Fonte: Nice Actimize

Volume de transações de tentativas de fraude	**+92%**
Porcentagem de tentativas de fraude	**+146%**

Sendo assim, a antifraude transacional apresenta-se como uma ferramenta que oferece uma camada adicional de proteção contra fraudes que possam acontecer em momentos sensíveis, analisando múltiplos fatores no momento da transação para detectar e prevenir possíveis ataques.

> **O Antifraude Pix da QI Tech apoia empresas e usuários a terem mais segurança em suas transações. Por sua relevância e eficiência, recebemos o prêmio FinTech e RegTech Global Awards por fornecer soluções inovadoras e fortalecer a segurança cibernética no setor financeiro".** Ricardo Alfaro – Sócio da QI Tech

A solução monitora e valida o valor de cada transação, verificando se ele está dentro dos parâmetros habituais para o usuário e alertando a empresa sobre transações que se desviam significativamente dos valores típicos. Transações envolvendo instituições desconhecidas ou suspeitas também são avaliadas como possíveis riscos para a operação.

Outro aspecto verificado é o horário da transação. Transações realizadas em horários atípicos para o usuário podem ser sinalizadas como potencialmente fraudulentas ao identificar comportamentos incomuns ou mudanças bruscas no padrão de transações, o que pode indicar tentativas de fraude. Por fim, a tecnologia utiliza informações como localização geográfica, dispositivos utilizados e métodos de autenticação para confirmar a autenticidade da transação, comparando essas informações com os dados cadastrados do usuário.

O motor de regras também trabalha junto com a antifraude transacional, permitindo que a empresa contratante escolha quais aspectos transacionais devem ser analisados para que sua operação continue funcionando de maneira segura. A empresa pode, por exemplo, definir horários específicos para a realização de transações, e aquelas realizadas fora desses horários predefinidos são bloqueadas ou submetidas a verificações adicionais, proporcionando uma camada extra de controle e segurança para os usuários.

Somente as transações que requerem uma análise manual ou "double check" devem ser encaminhadas para uma verificação adicional. Esse motor de regras opera em conjunto com a solução antifraude transacional, permitindo que a empresa determine quais aspectos transacionais devem ser analisados para garantir a segurança contínua das operações.

QI Sign Assinatura eletrônica com reconhecimento facial

Segundo a Global Industry Analysts, o mercado de assinaturas digitais deve alcançar US$ 48,2 bilhões até 2030, tendo um crescimento anual composto de 32,8% até 2030. A assinatura eletrônica é capaz de autenticar documentos digitalmente, eliminando a necessidade de papel e caneta. Regulamentada pela Lei 14.063/2020 no Brasil, a assinatura eletrônica é definida como "dados em formato eletrônico associados a outros dados eletrônicos, utilizados pelo signatário para assinar".

Uma assinatura eletrônica pode ter diferentes níveis de exigência, indo desde o nível mais simples - onde a assinatura pode ser realizada usando um login e senha ou um e-mail - até o nível avançado, que é o caso do **QI Sign.** Nesse nível, a assinatura do documento exige uma validação biométrica, e é aplicado em casos que envolvam informações sigilosas ou protegidas por lei.

O **QI Sign** utiliza o reconhecimento facial no processo da assinatura eletrônica, incluindo a captura e análise da imagem do rosto, convertida em dados numéricos únicos, comparados a uma base de dados biométricos para autenticação.

O processo de assinatura eletrônica é simples e rápido: O documento é enviado ao signatário via plataforma de assinatura, que notifica o usuário, verifica o conteúdo e insere dados de identidade. A plataforma gera uma assinatura eletrônica única, vinculada ao documento e ao signatário, registrando data, hora, localização e IP, criando uma trilha de auditoria.

As vantagens do reconhecimento facial incluem maior segurança e confiabilidade, praticidade e agilidade, além de redução de custos em comparação com assinaturas em papel, eliminando despesas como papel, administração de documentos e logística de contratos.

Sobre a QI Tech

Fundada em 2018, a QI Tech se consolidou como uma das principais fintechs do Brasil, oferecendo uma plataforma one-stop-shop de infraestrutura tecnológica e regulatória para serviços financeiros. A empresa permite que qualquer organização ofereça produtos financeiros aos seus clientes de maneira eficiente e segura.

A QI Tech destaca-se por sua área de Risk Solutions, que integra diversas camadas de segurança para garantir a integridade das transações financeiras, além de adotar rigorosos procedimentos de KYC (Conheça Seu Cliente), essenciais para a prevenção de fraudes e conformidade com as regulamentações. Esses procedimentos incluem a verificação detalhada da identidade dos clientes e a coleta de informações relevantes para garantir que os serviços financeiros sejam utilizados de forma segura e legítima.

+20 mi
de análises por mês

+90 mi
de cadastros validados

+R$60 bi
protegidos de fraudes

+120 mi
de rostos na base de faces

Entre em contato com os nossos especialistas

https://qitech.com.br/conheca-seu-cliente/#forms

Referências

Tecnologias Digitais Avançadas, Teletrabalho e Cibersegurança, da PINTEC Semestral 2022 - IBGE.

Occupational Fraud 2022: A Report to the Nations - ACFE (Association on Certified Fraud Examiners).

Atentados de fraude por minuto - Banco Central do Brasil.

2023 Visa Merchant Fraud Report - VISA.

Sumsub Identity Fraud Report 2023 - Sumsub.

Deepfakes: Real threat - KPMG e Reality Defender.

Inaugural Deepfakes in Business Report 2021 - Attestiv.

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000 - Forbes.

How AI is supercharging financial scams - Eureka Whittaker Macnaught.

Debunked: YouTube ads feature Elon Musk in deepfake videos pushing cryptocurrency scams - The Journal.

Identity Fraud Report 2024 - Onfido.

E-Commerce Trends 202 - Octadesk e Opinion Box.

The State of Enterprise Integration - Digibee.

2023 Fraud Insights Report - Nice Actimize.

Global Digital Signature Market to Reach US$50.6 Billion by 2030 - Market Research.com.

Value of NFT fraud plummets 82% in UK - RPC.

Financial Fraud Attack - Tessian.

Phishing, Insider Threats and Financial Losses Rise As User Awareness Stalls: A First Look at the 2023 State of the Phish Report - Proofpoint.

Consumer Sentinel Network - Federal Trade Comission.

42% dos brasileiros já foram vítimas do “golpe do Pix” - Money Report.

QITECH

Única empresa “as a service”
que atua de ponta a ponta como
infraestrutura tech e regulatória
para produtos financeiros.

qitech.com.br