INCOGNIA™

Fraude em tempos de COVID-19

Como estar à frente de fraudadores com novos métodos de verificação e autenticação de identidade

Sumário executivo

Este whitepaper foi criado pela Incognia para ajudar os líderes empresariais a terem uma perspectiva sobre os tipos de risco de fraude que estão aumentando durante a COVID-19, e a melhor forma de enfrentar os desafios atuais e futuros no novo normal. A pandemia da COVID-19, e o esforço para a sua contenção, aceleraram inesperadamente a transformação digital do nosso trabalho e das nossas vidas pessoais. O trabalho remoto introduziu questões de gestão de acesso a sistemas, pondo em risco a segurança da informação empresarial. Desprevenidas pela pandemia e suas consequências, as empresas que ainda não estavam, rapidamente voltaram seus esforços para o e-commerce e mobile commerce, levando uma quantidade muito maior de usuários para apps mobile. Os consumidores se voltaram para o comércio eletrônico como uma alternativa para não sair de casa, comprando de tudo, desde mantimentos até equipamentos fitness, a salvo do vírus, mas expostos ao risco de golpes de phishing e engenharia social, por exemplo. Além disso, o uso de pagamentos digitais e aplicativos bancários online aumentou à medida que se tornaram a solução para transações durante a pandemia. Esta mudança digital trouxe mais riscos de fraude à tona, pois os fraudadores aproveitam o caos para executar ataques mais frequentes e eficientes.

As empresas precisam reconhecer o aumento do risco de fraudes apresentado pela COVID-19 para implementar soluções inovadoras de verificação de identidade e autenticação seguras, que possam complementar e fortalecer as soluções existentes para estar à frente de fraudadores.

As mudanças de comportamento aceleradas pela COVID-19 vieram para ficar. Os profissionais de negócios e segurança precisam estar conscientes das novas ameaças às suas organizações e usuários mobile, se pretendem ficar à frente dos fraudadores.

Fraude em tempos de COVID-19

Como estar à frente de fraudadores com novos métodos de verificação e autenticação de identidade

Nos primeiros minutos de 2020, nem o maior visionário entre os futuristas poderia ter previsto como a dinâmica da sociedade iria mudar este ano. Ameaçados por um novo coronavírus sem cura, todos os países foram forçados a adotar rapidamente medidas de isolamento social. Álcool em gel e máscaras faciais bruscamente viraram a regra, e todos os que podem trabalhar de casa foram forçados a fazê-lo. Esta nova doença acelerou a mudança para o trabalho remoto e as transações digitais, permitindo às pessoas evitarem o contato, ficando em casa.

Funcionários de empresas tiveram que adotar o home office com velocidade recorde para os negócios continuarem funcionando, afrouxando as restrições de segurança por necessidade e se expondo a mais riscos. Com as pessoas trabalhando em casa em redes menos seguras, os dados das empresas ficam mais vulneráveis a ataques. Sem as configurações de segurança de seus escritórios, os profissionais de segurança e risco estão lidando com os desafios de um novo ambiente de trabalho que pode estar impactando a produtividade.

Rapidamente, os consumidores se voltaram para as transações mobile para fazer compras na segurança de suas casas. Para cumprir as regras de isolamento social, as pessoas começaram a fazer compras online de tudo, desde alimentos e artigos de higiene até produtos de lazer e equipamentos de ginástica. Transações financeiras de todos os tipos foram feitas digitalmente, acelerando a adoção de pagamentos digitais. Desde o início da COVID-19, as projeções de uso de pagamentos digitais têm aumentado, e agora espera-se que atinjam 67% de todas as transações até 2025 [1].

Desde o início da COVID-19, as projeções de uso de pagamentos digitais têm aumentado, e agora espera-se que atinjam 67% de todas as transações até 2025 [1].

[1] Bain & Company, *The Covid-19 Tipping Point for Digital Payments* (April 2020)

Transações sem dinheiro em espécie, feitas com tecnologias contactless, como a NFC, pagamentos digitais e serviços bancários online tiveram um pico no uso. Nos EUA, a Visa e Mastercard aumentaram seus limites de transação para pagamentos por aproximação [2]. No Brasil, apps como PicPay tiveram aumento muito expressivo de base de usuários [3], e segundo pesquisa da Mastercard, 69% dos brasileiros afirmaram que a COVID-19 os incentivou a utilizar pagamentos por aproximação [4].
Fica claro que o pagamento mobile se tornou uma das alternativas para transações seguras e sem riscos à saúde em meio a esta pandemia.

69% dos brasileiros afirmaram que a COVID-19 os incentivou a utilizar pagamentos por aproximação [4]

Esta transformação digital súbita está impulsionando uma necessidade sem precedentes de acelerar a adoção de novos métodos de comprovação de identidade e autenticação para permitir que as empresas combatam a fraude. Os desafios que estes aplicativos e instituições financeiras estão enfrentando para identificar um grande número de novos usuários e autenticar tantas transações de uma só vez são menos discutidos. Considerando que muitas empresas não tinham as defesas adequadas para fazer o scoring e identificar transações fraudulentas em apps mobile, a fraude neste tipo de transação tem aumentado consideravelmente.

> “Decisões que em tempos normais poderiam levar anos de deliberação são tomadas em questão de horas. Tecnologias imaturas e até perigosas são pressionadas para entrar em uso, porque os riscos de não fazer nada são maiores.”
>
> Destaca Yuval Noah Harari

[2] Oliver Wyman, *Payment Shifts with COVID-19.* (April 2020)
[3] Forbes, *Acelerada por isolamento PicPay chega a 20 milhões de clientes* (Maio 2020)
[4] Mastercard, *Pagamentos por aproximação e carteiras digitais* (Maio 2020)

Como disse o historiador Yuval Noah Harari em seu artigo no Financial Times [5], a tempestade passará e a maioria de nós ainda estará viva, mas viveremos em um mundo completamente diferente. Como a sociedade enfrenta todas essas mudanças e lida com os vários desafios da transição para os canais digitais, novos riscos estão surgindo. Infelizmente, à medida que o mundo avança, o mesmo acontece com os fraudadores. Eles se aproveitam do caos e da vulnerabilidade. Uma vez que a mudança de cultura para o home office foi inesperada e precisava ser implementada rapidamente, parte dela pode ter sido feita de maneira insegura. A falta de foco e atenção das pessoas durante este momento tão desafiador as torna mais vulneráveis às fraudes de roubo de conta, por exemplo, iniciadas com golpes de phishing mobile e engenharia social.

Sabendo disso, os especialistas devem estar atentos a novos métodos de verificação de identidade. As preocupações com a saúde e a rápida mudança para o digital criaram a necessidade de adoção de maneiras novas e criativas de autenticar o acesso a contas. Este whitepaper foi criado pela Incognia para ajudar os líderes empresariais a terem uma percepção dos tipos de risco de fraude que estão surgindo, e de como enfrentar melhor os desafios futuros.

A fraude está crescendo com a COVID-19

Os infratores se alimentam do caos e da confusão. O repentino avanço para o digital causado pela COVID-19 não é exceção, criando o tumulto perfeito para os golpistas, que estão encontrando maneiras de usar o distúrbio pandêmico a seu favor. Infelizmente, espera-se que a fraude aumente nas semanas e meses vindouros. À medida que o e-commerce e mobile commerce se tornam os canais de venda dominantes, os emissores de cartões de crédito e as empresas de varejo eletrônico relaxaram seus controles de fraude e aumentam os limites das transações a fim de evitar a criação de fricção para os usuários de apps.

As instituições financeiras haviam previsto anteriormente uma redução de 8% nas fraudes em 2020, mas projetam agora um aumento de 10% a 15% nas fraudes este ano [6].

Considerando o ambiente, os líderes empresariais devem estar em alerta máximo para um aumento das seguintes atividades fraudulentas:

[5] Yuval Noah Harari, *The world after Coronavirus* (Financial Times, Março 2020)
[6] Aite Group, *Workplace distancing: Adapting Fraud and AML Operations to COVID-19* (Abril 2020)

Golpes de engenharia social

Os ataques de phishing estão em ascensão durante a COVID-19 com fraudadores tirando vantagem das pessoas estarem distraídas. Estes golpes são concebidos para manipular as pessoas a realizarem uma ação ou fornecerem informações pessoais e ocorrem em vários canais, tipicamente Whatsapp, SMS, redes sociais e via e-mail. As informações obtidas através destes golpes resultam em outras formas de fraude incluindo fraude de identidade, roubo de conta e transação com cartão não presente (CNP).

Fraude na abertura de conta

Durante a COVID-19, os fraudadores estão tirando vantagem da confusão para abrir novas contas de forma fraudulenta. Neste caso, um fraudador usa informações pessoais roubadas, ou compradas na deepweb para abrir uma nova conta bancária, cartão de crédito, ou empréstimo pessoal. Aplicações para cartão de crédito fraudulento são o tipo mais comum de fraude de cartão de crédito nos EUA (88% de crescimento ao ano, como indicado pela Ascent [7]).

Fraude interna

A fraude interna é sempre uma preocupação durante tempos de recessão e o risco é maior durante a COVID-19 com a súbita transição para uma força de trabalho remota.

Também conhecida como fraude ocupacional, a fraude interna é geralmente cometida por indivíduos, contra as organizações que os emprega e assume a forma de roubo, exposição ou venda de informações confidenciais.

Roubo de conta

Um aumento significativo nos ataques de phishing durante a COVID-19, combinado com o fato de que muitas instituições estão flexibilizando seus métodos de comprovação de identidade e autenticação para oferecer uma experiência com menos fricção, tem aumentado as fraudes de roubo de conta. Os fraudadores geralmente assumem as contas para fazer compras e/ou transferir valores financeiros.

Cartão não presente (CNP)

Medidas de isolamento social implementadas durante a COVID-19 aumentaram as transações com Cartão Não Presente. Muitas pessoas estão comprando à distância - online, seja pelo celular ou computador - sem utilizar um cartão físico. Os fraudadores estão tirando proveito deste novo comportamento para misturar atividades fraudulentas com as de consumidores idôneos.

SIM swap ou troca de chip

O uso de autenticação de dois fatores (2FA) cresce, assim como as técnicas para burlar este método de segurança. Troca de SIM - ou SIM Swap - e SMS falsos, estão se tornando mais comuns.

Os fraudadores utilizam estes tipos de ataques para interceptar senhas temporárias, enviadas ao clicar no famoso recurso "esqueci minha senha", além da quebra de outros recursos de segurança de contas.

Fraude no auxílio emergencial da COVID-19

Governos de todo o mundo estão cedendo pagamentos emergenciais para o alívio econômico na crise do coronavírus, além de programas econômicos para ajudar as pequenas empresas a sobreviverem à pandemia. Nos EUA, mais de 4.000 websites maliciosos foram criados para tirar proveito de pessoas e empresas a procura de apoio governamental.

No Brasil, foram mais de 8 milhões de pessoas recebendo o auxílio indevidamente. Os fraudadores estão usando identidades sintéticas e roubadas para roubar estes pagamentos de subsídios.

Roubo de identidade

2019 foi o pior ano da história para fraudes com roubo de identidade de acordo com os dados da Ascent [8]. Gerações Xe Y são o alvo principal, já que eles têm mais crédito e tendem a fazer mais compras online, como afirma a Experian [9]. A maior parte das fraudes de identidade são relacionadas a cartões de crédito e outros empréstimos, mas roubo de informações pessoais, tais como carteira de motorista, endereços ou números de CPF, estão possibilitando novas formas de fraude de identidade, como a criação de identidades sintéticas concebidas para burlar métodos de verificação identidade.

[7] The Ascent, *Identity Theft Credit Card Fraud Statistics* (Abril 2020)
[8] The Ascent, *Identity Theft Credit Card Fraud Statistics* (Abril 2020)
[9] Experian, *Identity Theft Statistics* (Março 2018)

Mobile é o novo canal para ataques

Com a mudança acelerada para o digital, as transações, mais do que nunca, estão ocorrendo em dispositivos mobile. Em 2019, 53% do tráfego da web em todo o mundo veio de dispositivos móveis. O uso de smartphones não é mais apenas para jogos e mídias sociais. Nos EUA, mais de 63% dos usuários de smartphones têm pelo menos um aplicativo financeiro e mais de 55% têm pelo menos um aplicativo bancário instalado. No Brasil também temos números impressionantes: 65% dos brasileiros usam o celular para serviços bancários [10], e 90% de todos os acessos bancários pela internet, são feitos pelo celular [11].

65% dos brasileiros usam o celular para serviços bancários [10], e 90% de todos os acessos bancários pela internet, são feitos pelo celular [11].

Com uma parcela tão relevante da vida, principalmente financeira, acontecendo pelo celular, não é surpreendente ver fraudadores escolhendo o mobile com o principal canal para ataques. De acordo com um relatório da LexisNexis [12], os ataques em celulares cresceram 56% em 2019, enquanto os ataques em desktops caíram 23%, confirmando a crescente mudança do foco das fraudes para o mobile. Infelizmente, os golpistas não são atraídos apenas pela mobilidade devido a sua crescente relevância, mas porque ela ainda está repleta de vulnerabilidades de segurança. No Relatório de Segurança 2020 da Intertrust sobre Apps Mobile Financeiros nos EUA [13], observou-se que 71% dos apps de serviços financeiros tinham pelo menos uma vulnerabilidade de segurança de nível alto, um tipo de brecha que pode ser facilmente explorado e tem o potencial de danos ou perdas muito significativos. Em 2019, as tentativas de fraude aumentaram significativamente, com mais de duas vezes o número de tentativas de fraude e um aumento de 85% nas taxas de sucesso de fraude [14].

Em 2019, as tentativas de fraude aumentaram significativamente, com mais de duas vezes o número de tentativas de fraude e um aumento de 85% nas taxas de sucesso de fraude [14].

[10] IDC, *Serviços bancários por celular são acessados por 65% dos brasileiros* (Outubro 2019)
[11] Comscore, *90% dos acessos bancários são feitos por celular no Brasil* (Maio 2020)
[12] LexisNexis, *Cybercrime Report* (Março 2020)
[13] Intertrust, *2020 Security Report on US Financial Mobile Apps* (Junho 2020)
[14] LexisNexis, *Cybercrime Report* (Março 2020)

Isto representa uma enorme carga financeira para as instituições financeiras, dado que cada 1 dólar de fraude, gera um custo de 3,25 dólares em perdas relacionadas ao valor da transação, taxas e mão-de-obra investigativa. Mas há esperança, a Intertrust destaca que quase 70% de todas as ameaças de alto nível poderiam ter sido mitigadas utilizando proteções nativas para aplicativos mobile.

Ataques

+56%
mobile

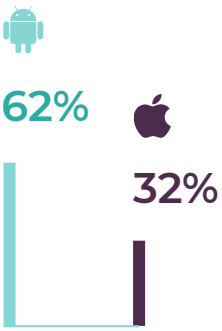
-23%
desktop

Vulnerabilidade de apps mobile

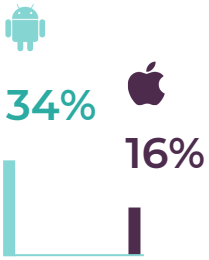
71%
tem pelo menos uma vulnerabilidade

82%
tem incriptação fraca

Vulnerável a extração da chave de encriptação



Comunicação insegura entre apps e servidores



O futuro é mobile, portanto, as empresas precisam priorizar novos tipos de verificação e autenticação de identidade que são construídos especificamente para este canal. As soluções de segurança mobile-first e para apps que equilibrem a fricção para usuários e uma segurança robusta para a conta serão fundamentais para evitar os danos corporativos e pessoais criados pela fraude. A Autenticação de Dois Fatores (2FA) adiciona uma forte camada de segurança, mas sua fricção inerente faz com que os usuários não queiram usá-la.

Em uma pesquisa recente da Duo Security, apenas 53% dos usuários pesquisados atualmente usam o 2FA, apesar dos benefícios óbvios em termos de segurança [15]. Uma abordagem mobile-first do 2FA que pode funcionar em segundo plano, baseando-se no comportamento do usuário para identificar e autenticar o acesso, provavelmente terá um impacto maior na redução da fraude, dado que não gera fricção. As empresas que oferecem uma experiência segura e agradável para os usuários de celulares são as que têm melhores condições para evitar fraudes, enquanto protegem seus negócios e clientes.

Em uma pesquisa recente da Duo Security, apenas 53% dos usuários pesquisados atualmente usam o 2FA, apesar dos benefícios óbvios em termos de segurança [15].

Como enfrentar os desafios de fraude

Os fraudadores estão sempre descobrindo novos vetores de ataque e aprendendo a aproveitá-los, trazendo desafios constantes para os especialistas em segurança e risco. Felizmente, novas tecnologias trazem novos métodos de verificação de identidade e autenticação para frustrar esses ataques e manter consumidores e empresas seguros.

Embora quase todas as soluções de segurança sejam eventualmente hackeáveis, a identidade e métodos de autenticação baseados em comportamento têm certas características que os tornam mais difíceis de serem quebrados. Ao contrário das soluções baseadas em credenciais estáticas, as soluções de biometria comportamental são dinâmicas e continuamente atualizadas, tornando-as difíceis - para não dizer impossíveis - de serem previstas, falsificadas ou forjadas pelos fraudadores.

Durante a COVID-19, a verificação de identidade é um grande desafio. Dado que os as pessoas não estão apenas trabalhando, mas também vivendo sua vida diária remotamente, mesmo após a reabertura da economia física, a capacidade de comprovar a identidade tornou-se crucial para o onboarding eficaz de clientes e o combate à fraude nas transações.

[15] Duo Security, *2019 State of Auth Report* (Dezembro, 2019)

Para a verificação de identidade, as empresas geralmente trabalham com empresas terceiras que se baseiam em informações publicamente disponíveis desatualizadas, muitas vezes levando a resultados falsos e revisões manuais que aumentam o atrito. A biometria comportamental oferece um método de verificação de identidade que compara informações pessoais com o comportamento no mundo real, sem exigir documentação, além de ser mais confiável e impor zero fricção para o usuário. Novas tecnologias como esta aumentam as conversões e a segurança ao mesmo tempo.

Para autenticação, especialistas em segurança recomendam fortemente o uso de autenticação multi-fator para proteger contas digitais. O acesso é concedido somente depois de autenticar com sucesso usando duas ou mais comprovações do usuário, onde cada uma representa "algo que eles sabem" (geralmente uma senha), "algo que eles têm" (como um smartphone com token) e "algo que eles são" (geralmente métodos biométricos, como uma impressão digital).

Hoje, nenhum método único é suficiente para manter as contas seguras. Com mais de 7 bilhões de registros expostos em vazamentos de dados somente entre 2018 e 2019, muitas senhas e outras informações importantes foram expostas, tornando-as não confiáveis

"Algo que você tem", como o celular, é suscetível a roubo. "Algo que você é" ou dados biométricos, são de longe o fator de autenticação mais forte, porém impressões digitais e reconhecimento facial já podem ser falsificados usando fotografias, deep-fakes, e até mesmo partes sintéticas simulando o corpo [16].

A chave para uma autenticação forte é combinar múltiplos fatores e estar sempre em busca de novas soluções que ainda não tenham sido hackeadas por fraudadores.

A autenticação por biometria comportamental é um dos novos métodos sem fricção usado para combater as fraudes.

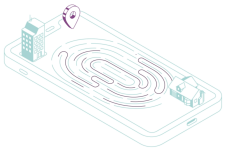
Ao utilizar um comportamento único, impossível de falsificar - como a cadência de digitação, o comportamento de localização ou mesmo a forma de caminhar de uma pessoa - a autenticação pode se beneficiar de uma camada adicional de segurança para evitar que os fraudadores tenham acesso.

[16] DW Shift, *How secure is Biometric Authentication Technology and Biometric Data?* (Dezembro, 2019)

Biometria comportamental baseada em localização

Incognia é um exemplo de uma solução de biometria comportamental baseada no comportamento de localização. Incognia usa dados de localização capturados de sinais de rede e sensores no dispositivo para identificar e continuamente validar o padrão de comportamento dos usuários. Usando padrões de localização em vez de informações pessoais estáticas, os usuários estão sempre seguros, além de protegidos contra fraudes, sua privacidade também está assegurada, mesmo na ocasião de um evento de vazamento de dados. Através de sinais de rede e em sensores de dispositivos, a Incognia constrói um perfil comportamental único para verificação e autenticação de identidade.

Como funciona



Fingerprint de Localização

Cria uma identidade digital privada baseada em padrões de comportamento de localização, únicos para cada usuário

Verificação de Endereço

Analisa o comportamento de localização para confirmar se os usuários realmente moram nos endereços fornecidos durante o onboarding do cliente no app

Localização Confiável

Verifica a localização de um dispositivo no exato momento em que uma ação importante no app é feita, como login ou pagamento

Integridade de Device

Detecta tentativas de enviar dados de localização forjados, falsificados ou emulados para apps mobile. Detecta até Android rooteado e Jailbreak de iOS.

Benefícios da Biometria de Localização

Identidade digital dinâmica e autenticação adaptativa

Detecção contínua de fraudes em tempo real

Sem fricção e não requer nenhuma ação dos usuários

Não identifica o usuário do app e protege seu anonimato

Aposte em estar simultaneamente seguro e em conformidade com a privacidade

Algumas medidas de segurança de contas invadem inadvertidamente a privacidade das pessoas. A privacidade do usuário tem sido um tema muito debatido e os relatórios de tendências, como o Tendências Fjord's [17] e 2020 Tech Trends da Future Today Institute [18], sugerem que a privacidade permanecerá um tópico crucial nos próximos anos.

Mais do que uma tendência, a privacidade é uma preocupação legal para empresas em todo o mundo.

Os governos estão desenvolvendo regulamentações para impor a proteção dos dados de seus cidadãos, tais como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR) na Europa e o Ato de Privacidade do Consumidor da Califórnia (CCPA) nos EUA, no Estado da Califórnia.

Segurança em camadas para combater a fraude

Especialistas em risco, segurança e governança sabem que não existe uma solução que seja bala de prata para a verificação e autenticação seguras de identidade. À medida que o mundo avança, infelizmente os fraudadores também avançam. Eles se aproveitam de vulnerabilidades, como as que o mundo tem enfrentado durante a COVID-19. Movimentos inesperados e carregados de insegurança, como tanta gente em home-office, a falta de foco e atenção das pessoas para evitar mensagens fraudulentas, a quantidade crescente de fake-news e a agitada mudança para transações digitais, tudo isso apresenta oportunidades de ouro para os golpistas.

Para combater os fraudadores e proteger as empresas, os líderes empresariais precisam estar cientes de que uma única comprovação ("algo que você tem") não é suficiente para garantir sistemas seguros. Como a necessidade de métodos de autenticação de dois fatores (2FA) aumenta mesmo que os usuários se adaptem, os fraudadores continuarão a encontrar caminhos.

As empresas precisam de múltiplas soluções para proteger as contas digitais contra fraudes.

[17] Accenture Interactive, *Fjord Trends 2020 Report* (2020)
[18] Future Today Institute, *2020 Tech Trends* (Março 2020)

6 Dicas fundamentais para combater a fraude durante a COVID-19

01

Adote o trabalho remoto e planeje a sua continuidade.
Atualize os protocolos de segurança remota e o sistema de gerenciamento de identidade e acesso para o novo normal, de funcionários em home office. Dê aos funcionários as ferramentas necessárias e treine-os sobre as melhores práticas.

02

Invista em soluções mobile-first.
À medida que os smartphones já são o núcleo da vida digital, esteja preparado para oferecer um método sem fricção para identificar e autenticar o acesso através de dispositivos móveis. Procure soluções biométricas comportamentais mobile-first para proteger seus usuários contra fraudes.

03

Construa camadas de soluções de segurança contra fraudes.
Prepare-se para ataques de fraude em diversos canais. Embora os fraudadores tenham um modus operandi preferido, eles tendem a capitalizar aonde perceberem uma nova oportunidade.. Prefira a prevenção à fraude com uma abordagem multi-níveis.

04

Procure por uma solução de segurança para transações sem fricção.
À medida que os limites são flexibilizados durante estes tempos desafiadores, explore formas de aumentar a segurança das transações mantendo uma boa experiência para o cliente para não perdê-lo para a concorrência.

05

Explore novas tecnologias de verificação de identidade e autenticação.
Soluções de segurança baseadas em comportamento podem ser sobrepostas às soluções de fraude existentes para proporcionar segurança adicional e monitoramento contínuo de riscos sem acrescentar fricção para o usuário.

06

Coloque a privacidade do usuário em primeiro lugar.
Saiba como novos métodos de fraude ameaçam a privacidade do usuário e tome medidas pró-ativas para protegê-lo e sua organização também. Garanta a conformidade de sua empresa com a LGPD.

Sobre a Inloco e Incognia

Inloco é uma empresa de identidade privada baseada na tecnologia de localização. Incognia é o produto que permite a prevenção de fraudes mobile para bancos, fintechs e e-commerces usando biometria comportamental baseada em localização, e oferece verificação e autenticação de identidade sem fricção. Temos sede em Recife e São Paulo, e nossa empresa-irmã que leva o mesmo nome do produto de prevenção à fraudes, Incognia, tem escritórios em Palo Alto e Nova Iorque. Temos atualmente mais de 60M+ de dispositivos com nossa tecnologia de localização.

Utilizamos dados comportamentais de localização para aumentar a segurança da conta de usuários, reduzir fraudes e fornecer serviços de localização privada sensíveis ao contexto. Nossa tecnologia utiliza sinais de rede e sensores no dispositivo para fornecer informações de localização altamente precisas. Ao construir um padrão de comportamento anônimo, único para cada usuário, Incognia fornece contexto de localização e cria uma identidade digital privada para a segurança das contas.

Empresas com aplicativos móveis e dispositivos conectados usam Incognia para verificação de identidade de usuários sem fricção, autenticação dinâmica adaptativa, avaliação de risco e detecção de fraude, tudo isso enquanto protegem a privacidade do usuário.

Privacidade

A privacidade do usuário é uma preocupação central da Inloco. A arquitetura de nossos produtos é feita sob os princípios do privacy by design, implementando técnicas de proteção da privacidade desde a concepção até o uso final de nossos produtos e soluções.

A tecnologia da Inloco foi projetada para impedir o acesso à informação capaz de re-identificar os usuários. Isto significa que a Inloco não coleta identificadores de dispositivos estáticos únicos (tais como IMEI e MAC), contas associadas (e-mail e telefone), dados de identificação civil (nome e número do seguro social), bem como alguns dados sensíveis como informações que revelam etnia, religião, opinião política, religião, filosofias, entidades políticas ou sindicais ou dados sobre saúde, vida sexual, genética e biometria física.

Nosso objetivo é, após tratamento, transformar os dados de localização em uma versão ilegível dos originais, para que ainda possam ser utilizados como a prova de conhecimento zero, mas não podem ser lidos sem uma chave de criptografia, ou, em certos casos, de forma alguma. Outras técnicas que usamos incluem uma estrutura de conjunto probabilística, privacidade diferencial e k-anonimato, aproximando os dados de uma anonimização completa.

Os dados coletados pela Inloco para oferecer seus serviços vêm do dispositivo móvel através de nosso Software Development Kit (SDK). Cada aplicativo deve apresentar para seus usuários a Política de Privacidade da Inloco em seus próprios Termos e Condições de Uso e Políticas de Privacidade, informando que os dados serão coletados pela Inloco. Uma vez autorizado, nosso SDK começa a coletar os dados sem identificar os usuários. Os usuários também podem negar a coleta de dados optando por não permitir e não dando consentimento, o que desativa os recursos para eles. Além disso, cada aplicativo deve permitir que os usuários optem por não coletar os dados a qualquer momento, dando aos usuários a propriedade de seus dados.

A equipe da Inloco compreende o poder e a sensibilidade dos dados de localização e é por isso que temos um compromisso interno de ir muito além para manter a proteção da privacidade do usuário.