2021, o ano dos maiores vazamentos de dados no Brasil

Guia de sobrevivência para gestores de risco

INCOGNIA™

Sumário executivo

2021 já pode ser considerado o ano do vazamento de dados no Brasil. Em um intervalo de menos de 1 mês, foram noticiados ao menos 3 grandes vazamentos de dados diversos de centenas de milhões de brasileiros. Apesar de estarem sendo noticiados agora, nem todos os vazamentos aconteceram este ano, mas se tornaram notórios após o mega vazamento que liberou os dados de mais de 223 milhões de pessoas. Somam-se a esses os 270 milhões de registros da Dataprev, e os dados de mais de 100 milhões de clientes, supostamente de empresas de telefonia.

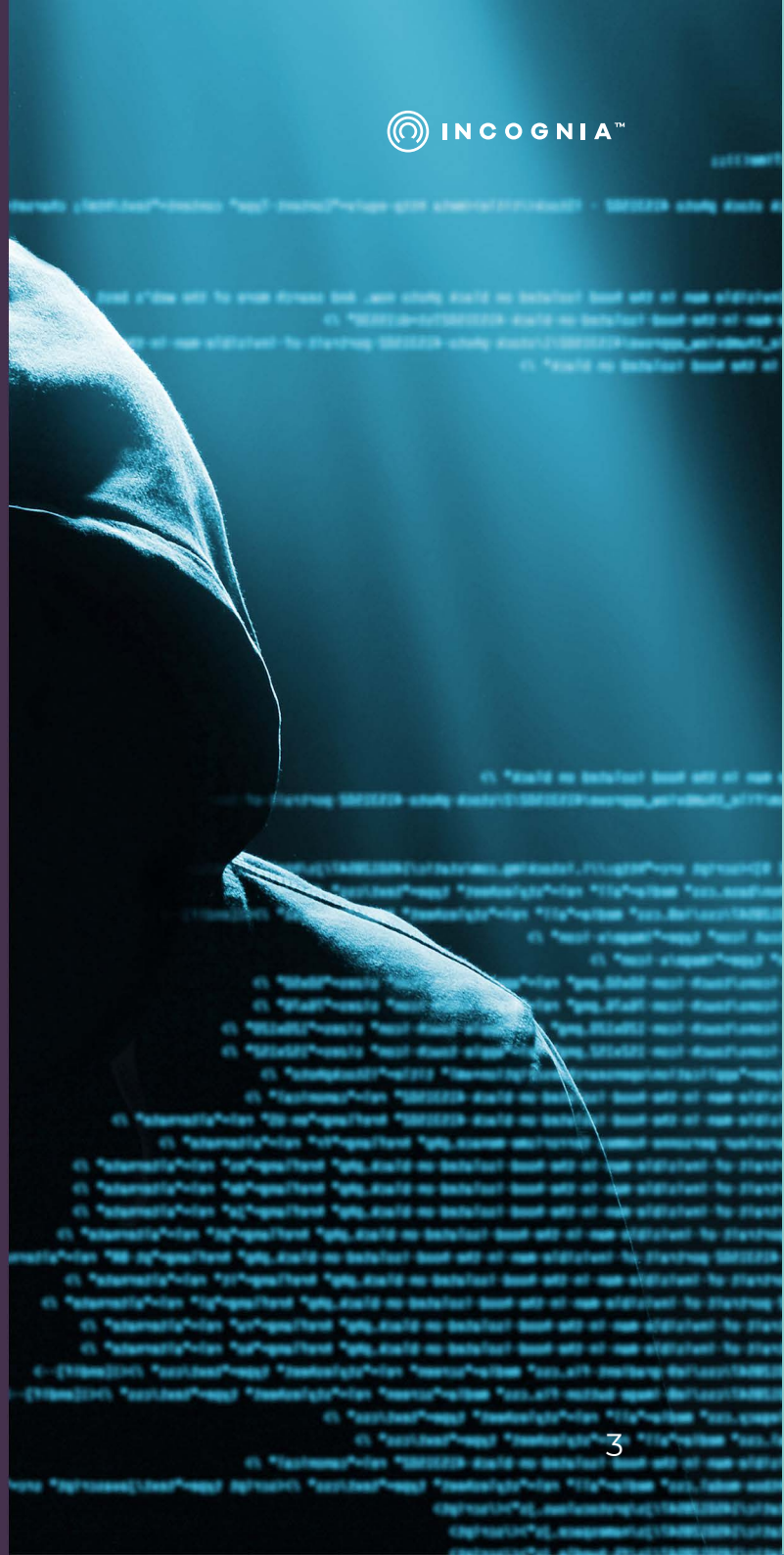
O número de fraudes deve aumentar exponencialmente daqui pra frente, dada a natureza desse tipo de informação. As consequências para as instituições e a população têm potencial para ser desastrosas, com efeitos e prejuízos que poderão ser sentidos por anos, uma vez que os dados já vazaram e estão disponíveis tanto na Deep Web, quanto publicamente, e em alguns casos, estes por si só apresentam fragilidades na proteção da população contra possíveis fraudes.

O que mais impressiona nos recentes episódios de vazamentos são a amplitude e a variedade de tipos de dados, que vão desde nome à foto do rosto (o nome do arquivo em JPG é o CPF do indivíduo!), CPF, nome dos pais, endereço, telefone, e-mail, score de crédito, salário, renda e muito mais. Estas informações são a maneira mais comumente utilizada para a verificação de identidade na abertura de novas contas e autenticação das que já existem, por meio de uma técnica chamada “checagem de pares”. Funciona de forma tão simples quanto o próprio nome diz: uma pessoa buscando abrir uma conta, ou realizar uma transação, apresenta uma informação credencial e a instituição checa se esse dado é real, de forma automática ou manual. A maneira mais amplamente utilizada é a checagem de pares com informações estáticas, realizada utilizando diferentes técnicas, tais como checagem de números de documentos, confrontar endereço de um comprovante de residência e o endereço de residência declarado e, mais recentemente, a famosa selfie, que pode detectar através de reconhecimento facial a correspondência entre um rosto e uma foto em um documento.

No material a seguir, serão descritos tipos de técnicas de prevenção à fraude que passarão a apresentar menos eficácia daqui para frente, além de explicar por que isso acontecerá, e quais alternativas apresentarão resultados confiáveis e mais consistentes com base neste novo cenário em que o Brasil se encontra.

Técnicas de fraude que tendem a aumentar

Os dados vazados são matéria-prima para muitas técnicas possíveis de fraude e estelionato, porém alguns golpes e métodos devem crescer mais rapidamente que outros.



Fraude na abertura de conta

Abertura de conta com identidade sintética

Com tantas informações reais de identificação da população à disposição, a abertura de conta com identidade sintética é um dos golpes que mais tende a crescer. Este tipo de fraude ocorre quando os fraudadores combinam dados de identidade legítimos e falsos para criar uma identidade falsa e "sintética". Podem ser usados o nome e o número do CPF legítimos de uma pessoa, o endereço de outra, e o número de telefone de outra. Os fraudadores usam esses elementos para criar uma pessoa fictícia e depois abrem novas contas em bancos ou em outras empresas on-line com estas credenciais. Eles realizarão negócios legítimos com essas contas durante meses ou mesmo anos, construindo um histórico idôneo com a identidade sintética com o propósito de aumentar seu score de crédito e eventualmente executar uma transação com um alto pagamento. Infelizmente, este é um tipo de fraude que é notoriamente difícil de ser detectada. De acordo com o Fed (equivalente ao Banco Central nos Estados Unidos), os modelos de detecção de fraude comumente usados falham na identificação da fraude de identidade sintética em 85% a 95% dos casos.

Cerca de 85% dos solicitantes de crédito identificados como potenciais fraudadores sintéticos não foram sinalizados como usuários de alto risco por modelos tradicionais antifraude, segundo pesquisa da ID Analytics.

Os processos de abertura de contas de instituições financeiras contam com a coleta de informações para identificar a identidade do potencial novo cliente. Muitas informações são obrigatórias no processo de KYC (Know Your Customer), como, por exemplo, a comprovação de endereço, que exige a validação de um documento, geralmente de contas de consumo. Porém, esse documento pode ser facilmente falsificado eletronicamente, permitindo que o processo seja concluído de forma fraudulenta.

Os modelos de detecção de fraude comumente usados falham na identificação da fraude de identidade sintética em 85% a 95% dos casos.

Fonte: FED

Este é um dos tipos de fraude que mais cresce, principalmente nos Estados Unidos, segundo estimativas da consultoria McKinsey. A crescente de casos está ligada à quantidade de vazamentos de dados, cada vez mais comuns com a ampliação de ambientes digitais. Afinal, para um cibercriminoso criar uma identidade sintética é preciso reunir informações verdadeiras, como documentos de pessoas físicas, geralmente abundantes nesses vazamentos.

Sem dúvida, com os recentes episódios de vazamentos de dados, este deve ser um dos tipos de técnica mais usados para viabilizar a abertura de novas contas bancárias de forma fraudulenta.

Falsificação de documentos

A falsificação de documentos como CNH e RG, necessários para identificação de um indivíduo que abre uma conta em banco digital, é bastante simples. De posse das informações de uma pessoa, todas já disponíveis amplamente após os vazamentos de dados, é possível criar documentos falsos por um custo relativamente baixo. No centro de São Paulo, um RG falso com alto grau de sofisticação na falsificação custa em torno de R$300. Basta um fraudador utilizar informações de pessoas reais e colocar outro rosto na foto, o mesmo que poderia usar para reconhecimento facial, e, assim, utilizar o documento falso para a abertura de conta em um banco digital.

Um RG falso com alto grau de sofisticação na falsificação custa em torno de R$300.

Roubo de conta

Engenharia Social

Fraudadores utilizam a engenharia social para roubar contas já existentes. Normalmente é feito contato com a vítima do golpe, por telefone, mensagem ou email, sendo que o golpista finge ser uma instituição ou serviço e pede a confirmação de dados e informações. Municiado de informações sensíveis e com conhecimento a respeito da vítima, ganham confiança para conseguir informações que faltam para invadir uma conta, como uma senha eletrônica, fornecida pela própria vítima. De posse da conta do usuário, no caso de uma instituição financeira por exemplo, o fraudador pode fazer transações, causando enormes prejuízos. O famoso golpe do whatsapp pode ser aplicado da mesma forma.

No início da pandemia, entre abril e junho de 2020, um em cada oito brasileiros havia sofrido uma tentativa de ataque de phishing, segundo relatório da Kaspersky. O estudo aponta que os criminosos se aproveitaram da situação para enviar e-mails e mensagens relacionadas à Covid-19 e programas de auxílio social, mostrando que esses golpes são estruturados de forma estratégica. O vazamento recente oferece aos compradores dos dados a oportunidade de traçar um perfil completo da vítima, incluindo nomes de familiares, o que facilita ainda mais na hora de escolher o alvo e a forma como manipular cada indivíduo.

As possibilidades são inúmeras. O criminoso pode entrar em contato com uma pessoa se passando por uma instituição, por exemplo, e solicitar dados aos quais ele não tem acesso (como uma senha eletrônica) ou até mesmo a confirmação de um código enviado por SMS e que, na verdade, será usado para passar pela autenticação de dois fatores de um aplicativo. O contrário também pode ocorrer: o agente mal-intencionado pode entrar em contato com uma instituição e, pelo fato de ter todos os dados pessoais do cliente, se passar facilmente pela vítima para fazer qualquer tipo de solicitação.

Entre abril e junho de 2020, um em cada oito brasileiros havia sofrido uma tentativa de ataque de phishing.

Fonte: Kaspersky.

Outra maneira engenhosa é, de posse das informações do usuário, o fraudador liga para um canal de atendimento ao consumidor, e se faz passar pelo titular da conta. Este tipo de golpe será potencializado com os recentes vazamentos, já que o golpista poderá fazer todas as confirmações às perguntas de um atendente, uma vez que tem um grande volume das informações essenciais que normalmente são usadas por clientes legítimos ao se identificarem para instituições.

SIM Swap

Com informações da população à disposição, fica mais fácil para um fraudador aplicar o golpe de SIM Swap. Aqui a engenharia social acontece quando um fraudador liga para uma operadora telefônica se passando pelo dono da linha, e pede transferência para um outro chip. Ele confirma todas as informações corretas do dono da linha, e tendo sucesso, tem o número do usuário à sua disposição. À partir deste momento, o fraudador pode roubar contas nas quais o usuário tem aquele número como chave para autenticação de dois fatores por SMS, por exemplo, que é presente na maior parte das contas, de email, e-commerce, redes sociais e até alguns serviços financeiros, como apps de investimentos. O fraudador pode, com o pedido e recebimento do SMS, redefinir as senhas das contas destes apps mobile e roubar a conta do usuário.

> O fraudador pode roubar contas nas quais o usuário tem aquele número como chave para autenticação de dois fatores por SMS.

Phishing

Ataques de phising mobile tendem a crescer, também para o roubo de conta. A vítima é induzida ao erro, clicando em URLs maliciosas que podem instalar malwares no telefone para roubar senhas, ou a vítima pode ainda ser levada a colocar suas informações em páginas falsas, incluindo suas senhas. Será mais fácil induzi-las ao erro, uma vez que verão suas informações reais e tenderão a confiar na legitimidade da instituição.

Métodos de prevenção à fraude que serão menos eficazes

Métodos baseados em informações estáticas perdem força

Informações estáticas, por definição, não mudam. Algumas delas são amplamente utilizadas em algumas das técnicas de prevenção à fraude do mercado, como a checagem de credenciais em bancos de dados. De posse de informações reais dos usuários, fraudadores poderão aplicar para a abertura de contas, e os métodos que consultam informações estáticas em bancos de dados, em tese, não saberiam diferenciar um fraudador de usuário legítimo, já que as informações fornecidas coincidem com as de uma pessoa idônea. Por esta razão, métodos de prevenção à fraude baseadas em informações estáticas serão pouco eficazes e confiáveis daqui para frente.

Verificação de identidade no onboarding

Algumas técnicas para a verificação de identidade já são tradicionalmente utilizadas no onboarding de usuários em aplicativos digitais de instituições financeiras. As técnicas abaixo, após o vazamento de dados, devem ser menos eficazes na prevenção de fraudes.

Validação de endereço com documento comprovante de residência

Neste método, os aplicativos pedem as informações de identificação civil de um indivíduo e a declaração de endereço de residência. As informações são então enviadas a um birô de crédito, por exemplo, que confirma em seu banco de dados a veracidade do cruzamento das informações fornecidas, e através da comparação de informação declarada com a informação previamente cadastrada no banco de dados.

Os métodos que consultam informações estáticas em bancos de dados, em tese, não saberiam diferenciar um fraudador de usuário legítimo, já que as informações fornecidas coincidem com as de uma pessoa idônea.

De posse do cruzamento de informações civis da população e seu endereço real de residência, é bastante simples para um fraudador falsificar uma conta de consumo. Assim, é possível com documentos falsos e todas as informações corretas, que irão coincidir com o dado de birôs de crédito, o fraudador ter sucesso na abertura de uma conta digital de um banco, por exemplo, que lhe fornecerá acesso a crédito instantaneamente em nome de outra pessoa.

Força de vínculo de variáveis informadas pelos clientes

Algumas técnicas de mercado atribuem uma nota de risco para um usuário fazendo a tentativa de abertura de nova conta tomando como base a força do vínculo entre informações como CPF, email, telefone e CEP. Estas informações estão facilmente disponíveis para fraudadores. Como a comparação de informações declaradas, que irão coincidir com a de pessoas reais em bancos de dados que serão consultados, irão ajudar em uma nota de risco efetiva? Esta técnica deve ser analisada com cuidado em face da nova realidade.

Verificação de identidade por atendentes em call centers

A autenticação de usuários, por vezes, ainda passa pelo atendimento humano feito por atendentes em call centers. Isto pode ser feito tanto para a abertura de contas quanto para autenticação de login, no caso de senhas perdidas, mudança de informações cadastrais, ou até confirmações de compra de transações em e-commerce. Esta verificação de informações pessoais é falha, dado que fraudadores têm acesso e podem com facilidade se passar por qualquer pessoa, apenas confirmando as perguntas feitas por um atendente. Para o atendimento por telefone poder continuar a ser usado como fator de segurança, deverá passar a contar com a biometria por reconhecimento de voz, que não é infalível, mas já é muito mais seguro do que verificação de identidade por meio de dados pessoais.

Reconhecimento facial sem *liveness detection*

O reconhecimento facial já é utilizado na maioria dos bancos mobile como técnica de verificação de uma pessoa. No entanto, já foi comprovado que fotos de pessoas são capazes de enganar algumas ferramentas de reconhecimento facial. Portanto o *liveness detection,* que exige que o usuário mexa a cabeça em determinada direção ou sorria, se torna essencial para que o reconhecimento facial se mantenha efetivo.

Autenticação

O uso de credenciais para reconhecer clientes com os quais as instituições já têm relacionamento mudará drasticamente ao longo dos próximos anos. Não só porque cada vez mais as empresas estão se dando conta de que os métodos atuais são pouco amigáveis, como pela necessidade de se lembrar de uma senha para cada serviço que usamos, mas também porque estão com sua eficácia comprometida, do ponto de vista de segurança na era dos vazamentos de dados.

> Empresas ainda usam SMS como 2FA, mesmo que, comprovadamente, não seja complexo burlar com engenharia social.

Senhas de uso único por SMS

São popularmente usadas em aplicativos mobile. É gerado aleatoriamente um número único, enviado por SMS para o telefone celular do titular da conta, para que o cliente possa inseri-lo em um formulário no aplicativo, demonstrando a propriedade (ou pelo menos o controle) de um dispositivo mobile previamente autenticado. O SMS baseado no 2FA pressupõe que o usuário possua as credenciais de login corretas e está de posse do telefone utilizado para receber o código de acesso único.

Nos recentes casos de vazamentos, os números de telefones celulares de usuários também vazaram. De posse de todas as informações de uma pessoa e seu número de celular, um fraudador consegue com certa facilidade aplicar a técnica de SIM Swap, na qual, por meio de engenharia social, é possível, via SAC das operadoras telefônicas, tomar posse da linha telefônica de uma pessoa.

O NIST (Instituto Nacional de Normas e Diretrizes Tecnológicas nos EUA) definiu o SMS como um método pouco seguro para autenticação de dois fatores em suas diretrizes 800-63 de Identidade Digital. Mesmo assim, tanto nos Estados Unidos quanto no Brasil, ainda é um método de 2FA comumente utilizado e oferecido aos usuários. Mesmo com órgãos como o NIST não recomendando o SMS como 2FA, por que este método ainda é comumente disponibilizado e utilizado? Uma das possibilidades é pelo SMS ainda ser uma das formas mais fáceis de compreensão do 2FA para um usuário.

As empresas estão dando prioridade à facilidade de uso e retirada de fricção, mesmo que o SMS, comprovadamente, não seja complexo de burlar com engenharia social.

Senhas

Senhas não são práticas para o usuário. Seu formato não é padronizado e é aconselhável que as pessoas, não só utilizem a maior quantidade de senhas diferentes possível, mas também altere-as com frequência para não serem impactadas em um episódio de vazamento de dados. Mesmo senhas fortes não impedem roubos de contas quando fraudadores usam malwares, engenharia social e phishing.

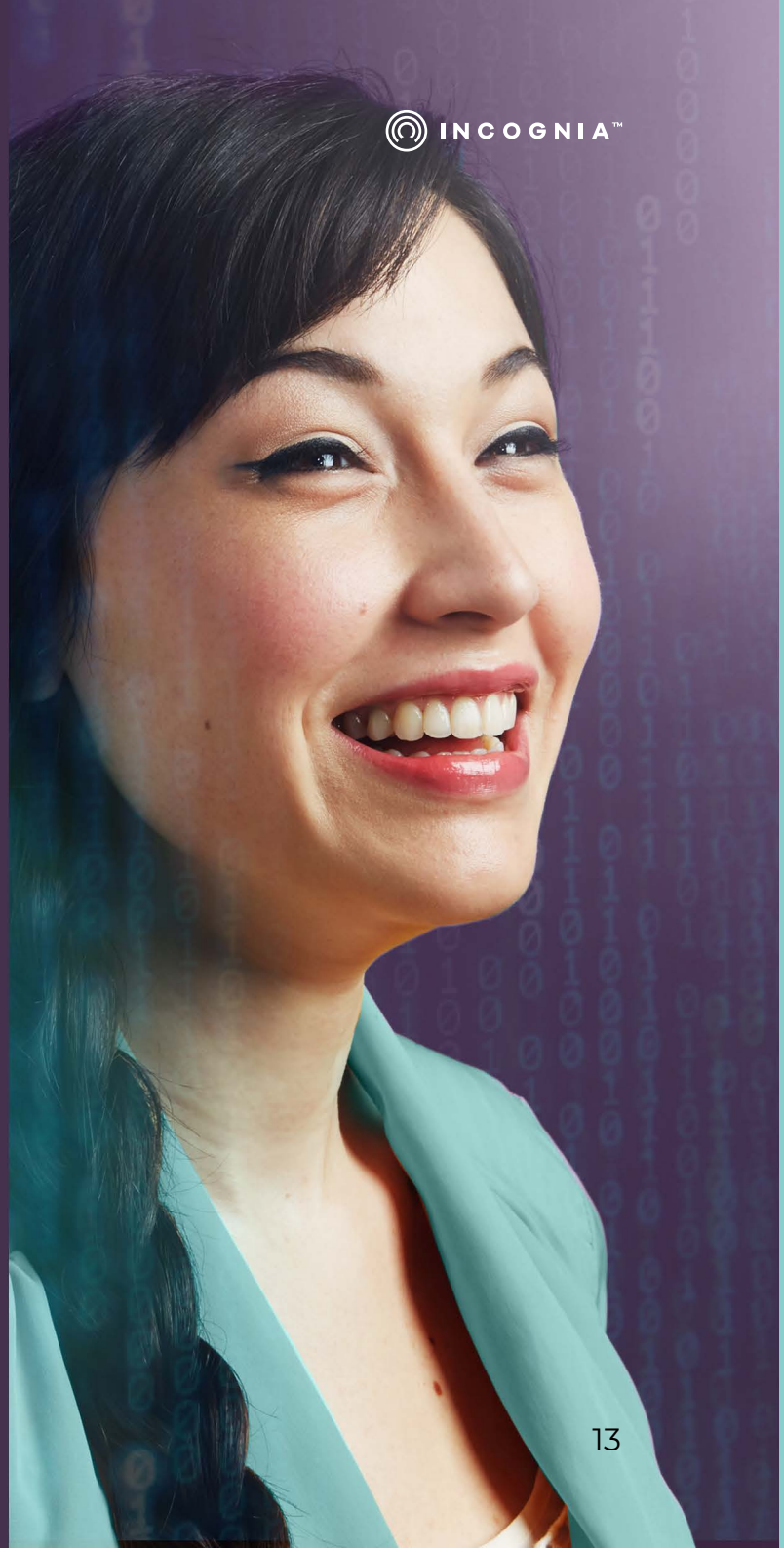
Se senhas são pouco práticas para usuários e inseguras, por que continuam sendo usadas como principal credencial de autenticação?

Knowledge-based authentication (KBA) / Perguntas de Conhecimento

São perguntas projetadas para exigir que o cliente introduza informações, em tese, não públicas e que só ele saberia, verificando assim, a identidade do cliente. Comumente são usadas perguntas como o nome dos pais, endereço, data de aniversário, CPF ou outras informações que normalmente só os usuários sabem, porém, após vazamentos de dados, as respostas a estas perguntas como fator de segurança estão altamente comprometidas, além de serem informações estáticas. Em muitas contas digitais, perguntas de conhecimento podem ser utilizadas em rotinas de recuperação de senhas. Com as informações pessoais da população à disposição, muitas respostas a perguntas, como por exemplo “Qual é o nome de sua mãe”, estão comprometidas como fator de segurança e técnica de recuperação de senha.

Se senhas são pouco práticas para usuários e inseguras, por que continuam sendo usadas como principal credencial de autenticação?

Como manter os clientes mobile protegidos na era dos vazamentos de dados



O que não fazer

01

Evite informações estáticas como principal comprovação de identidade.

Elas não protegerão usuários e instituições como uma vez fizeram as empresas e agentes do sistema financeiro que utilizam técnicas de prevenção à fraude dependentes de informações estáticas, como as descritas acima, estão se sujeitando a golpes de abertura de conta com identidades falsas e sintéticas e documentos falsos.

02

Evite mais SMS como 2FA

O número de telefone celular é fácil de ser clonado, além do NIST já ter declarado o SMS uma tecnologia pouco confiável como método de segurança para autenticação.

03

Evite mais senhas para a autenticação de usuários em seu aplicativo mobile

Senhas são inseguras e pioram a experiência de uso de aplicativos mobile. Ao retirar senhas como fator de autenticação de um usuário em um aplicativo, são eliminados os riscos atrelados a vazamentos de dados que incluem a identificação do usuário e sua senha, além de melhorar drasticamente a experiência do usuário. É necessário incluir outros métodos de autenticação, mas que não apresentem as mesmas fragilidades.

O que fazer

01

Use métodos com dados dinâmicos para verificar a identidade de usuários no onboarding

Dados dinâmicos mudam o tempo todo, pois usam o comportamento humano como base. Como o comportamento humano muda o tempo todo, é um alvo em movimento, tornando difícil, ou quase impossível para fraudadores utilizá-lo, mesmo após um possível episódio de vazamento desses dados. A biometria comportamental por localização é um exemplo de dado dinâmico. Nenhuma pessoa tem o comportamento de localização como o de outra, e isso garante a possibilidade de usar este comportamento como identidade. É uma forma de identidade complexa e em constante evolução, portanto é impossível de ser reproduzida ou forjada.

02

Use o comportamento do usuário para autenticá-lo ao invés de utilizar senhas

Ao retirar senhas como principal método de autenticação, é preciso incluir um substituto mais seguro. Ao usar o comportamento de localização do usuário, o aplicativo mobile garante uma boa experiência de uso, já que o usuário não precisaria realizar nenhuma ação, além de ser ele mesmo. Sua segurança seria mantida, já que os fraudadores não conseguiriam forjar seu comportamento de localização.

03

Adicione liveness detection no reconhecimento facial

Fotos da população também foram vazadas e estão atreladas às informações de identificação civil. Um fraudador pode facilmente falsificar documentos, e, porventura, fazer o face-match com uma foto, caso a tecnologia de reconhecimento facial não contar com o liveness detection. É uma tecnologia indispensável para apps mobile que usam reconhecimento facial.

04

Use reconhecimento de voz no processo de autenticação

Dentre os tipos de biometria, este talvez seja o menos explorado. Muitos serviços atualmente contam com atendimento eletrônico ou humano, que podem contar com senhas ou o pedido de informações pessoais para a identificação do usuário, o que fragiliza o processo de autenticação. Porém com tantas informações pessoais disponíveis para fraudadores, passará a ser uma tecnologia cada vez mais importante e relevante.

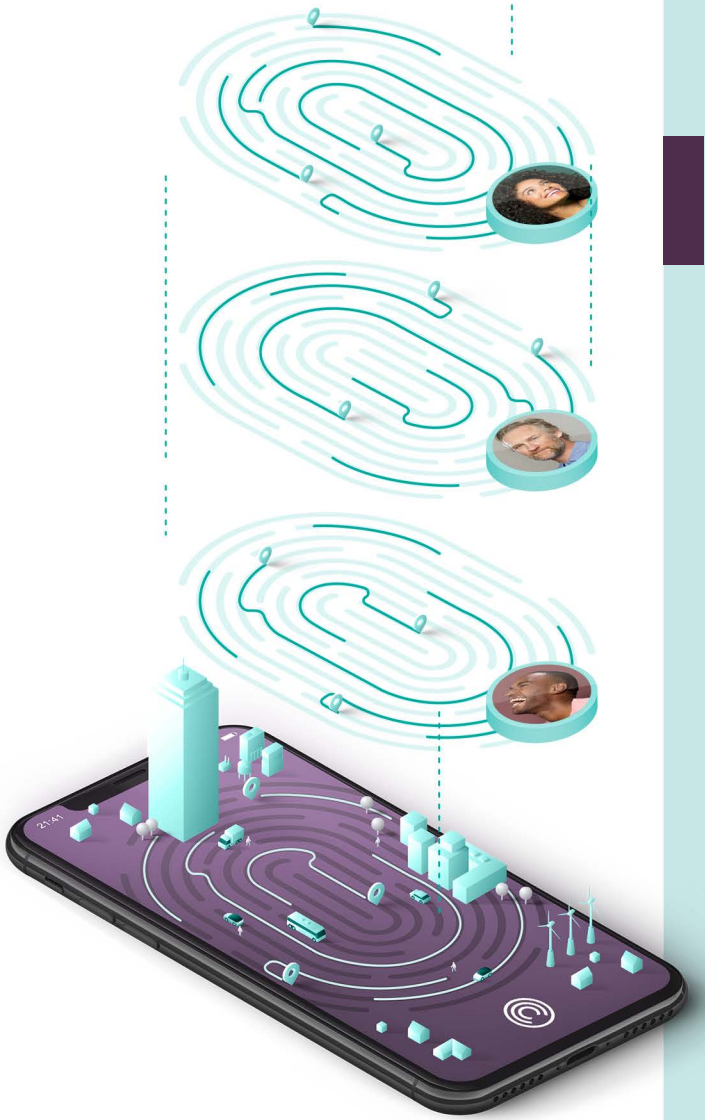
Conheça Incognia

Incognia é uma solução de identidade mobile sem fricção para bancos, fintechs e m-commerce, que permite verificação e autenticação em tempo real de usuários confiáveis e detecção de fraudadores, possibilitando aumento de receita através da aprovação superior de clientes legítimos, além de redução de custos associados à fraude e revisões manuais.

A identidade mobile de Incognia funciona através da biometria comportamental por localização.

Por que a biometria comportamental por localização é imune a vazamentos de dados?

A biometria comportamental por localização de Incognia utiliza a força de sinais de localização e sensores de movimento do dispositivo mobile para construir um fingerprint de localização para cada usuário baseado em seu respectivo comportamento de localização, que é único. Estas informações são encriptadas e hasheadas, e não podem ser utilizadas para identificar um usuário diretamente.



A identidade mobile de Incognia funciona através da biometria comportamental por localização.

Para abertura de novas contas em banco de varejo, Incognia **aumentou em 52% a aprovação automática** de contas no onboarding”

Em app de fintech, Incognia alcançou **99,9983% de assertividade** no processo de aprovação de logins

Conclusão

Quando dados estáticos vazam de bancos de dados, já não há mais o que fazer. Eles poderão ser utilizados por fraudadores e os usuários em geral não conseguirão mais alterar informações dessa natureza. Métodos de prevenção à fraude que utilizam dados estáticos têm eficácia e proteção inferiores. É por isso que vazamentos sem precedentes, como os que vimos no Brasil nos últimos meses, irão mudar radicalmente a forma como organizações tratam segurança e ferramentas de prevenção à fraude. Golpes como abertura de contas com identidade sintética, falsificação de documentos e roubo de conta com SIM Swap ou engenharia social tendem a aumentar, com o volume de dados disponíveis não só para fraudadores, mas para o público em geral em sites de fácil acesso. Senhas criadas pelos usuários também não são mais a melhor alternativa para a autenticação, já que são uma informação que os fraudadores podem ter acesso ao invadir uma conta ou em outros episódios de vazamentos.

Dados estáticos apresentam mais fragilidade para fazerem a verificação e autenticação de identidade, já que uma vez em posse de fraudadores, não podem ser alterados, e instituições não podem assegurar quem está fornecendo tais informações. Dados dinâmicos são mais confiáveis, já que são mais difíceis de copiar, forjar, e quando são baseados em comportamento, são constantemente atualizados, de acordo com o perfil de localização e atividades dos usuários.

Entendas profundamente as soluções de Incognia

Conheça o onboarding ágil ⟶

Saiba mais sobre a autenticação baseada em risco ⟶

© 2021 Incognia All Rights Reserved