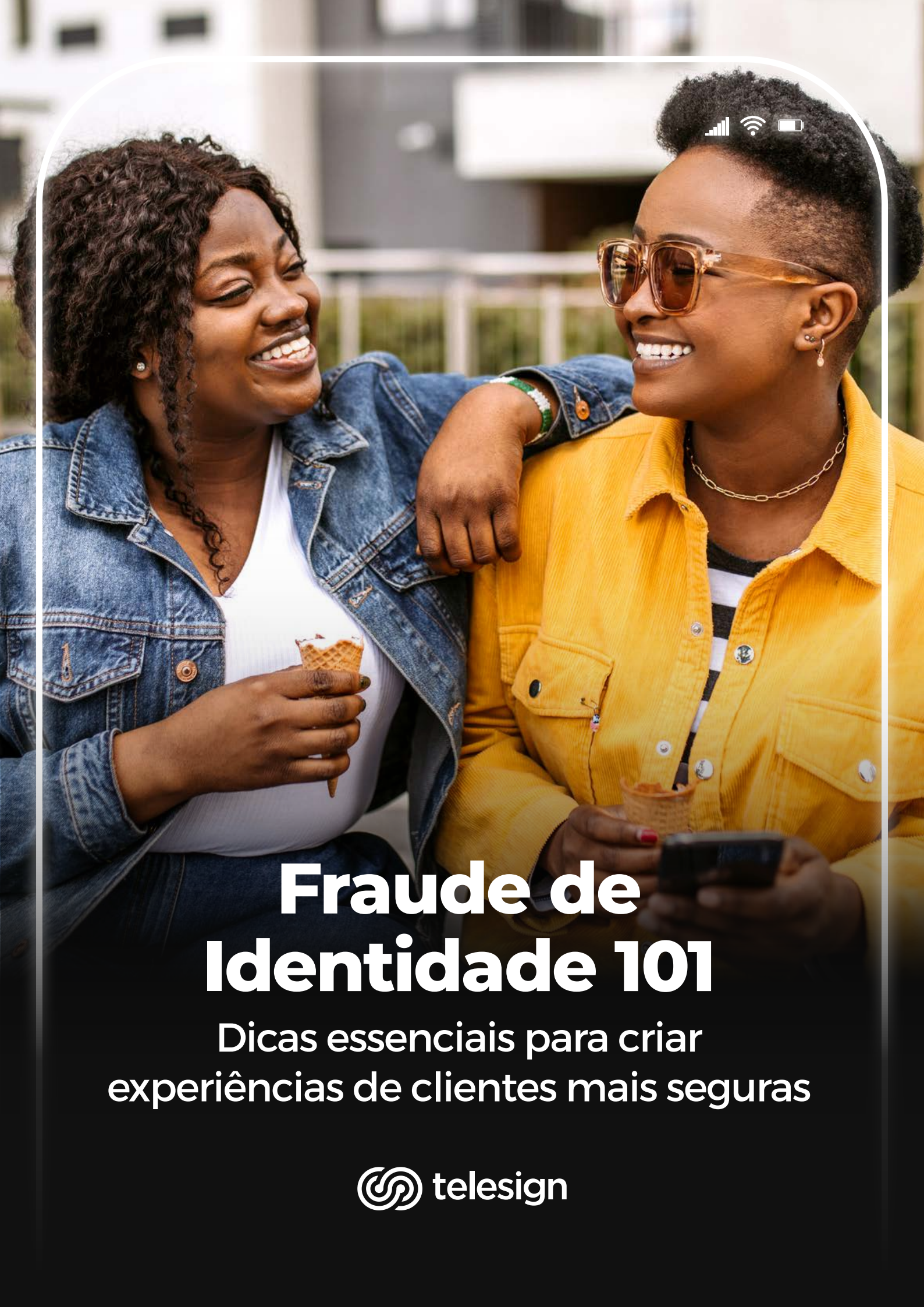


Fraude de Identidade 101

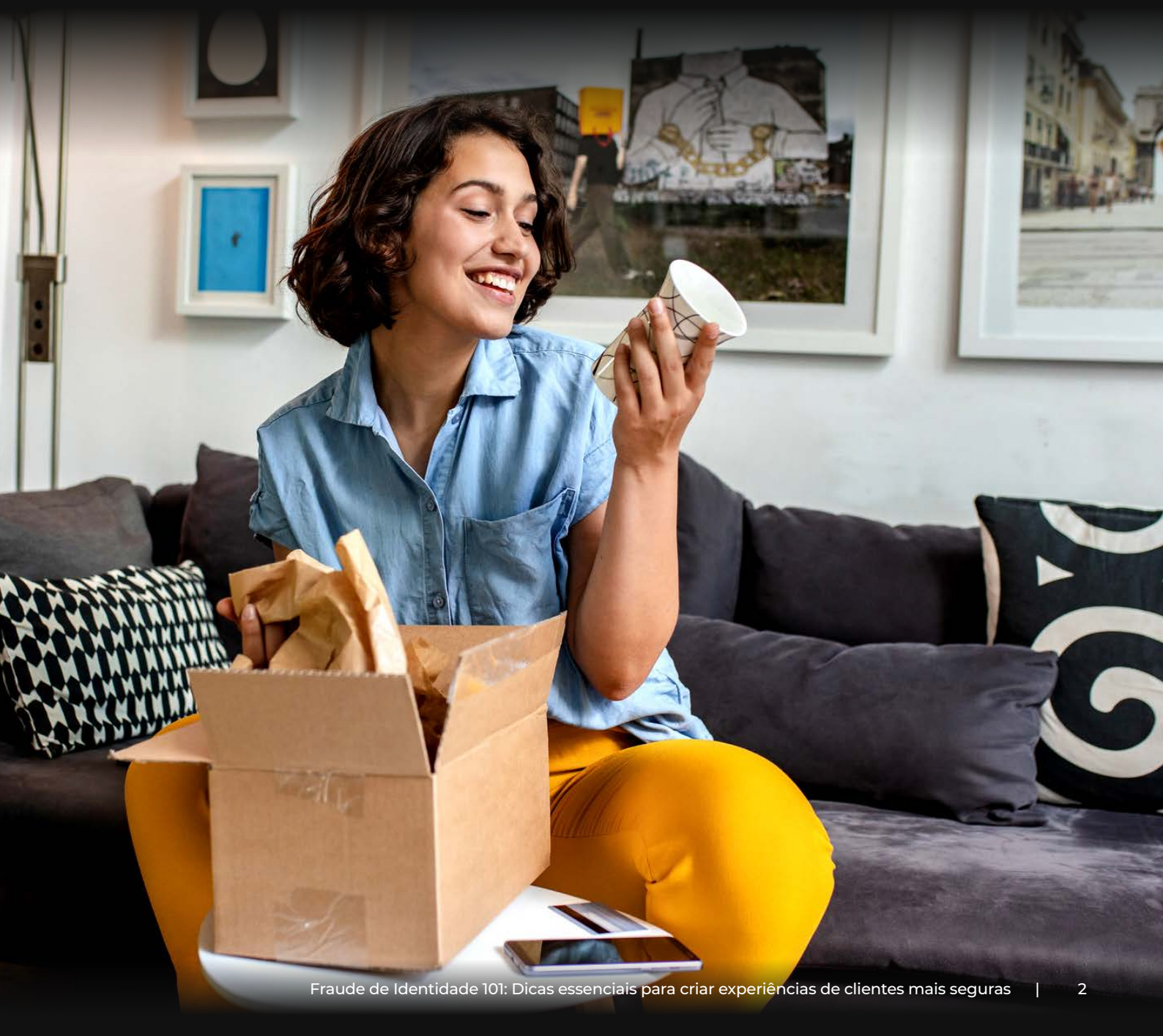
Dicas essenciais para criar experiências de clientes mais seguras

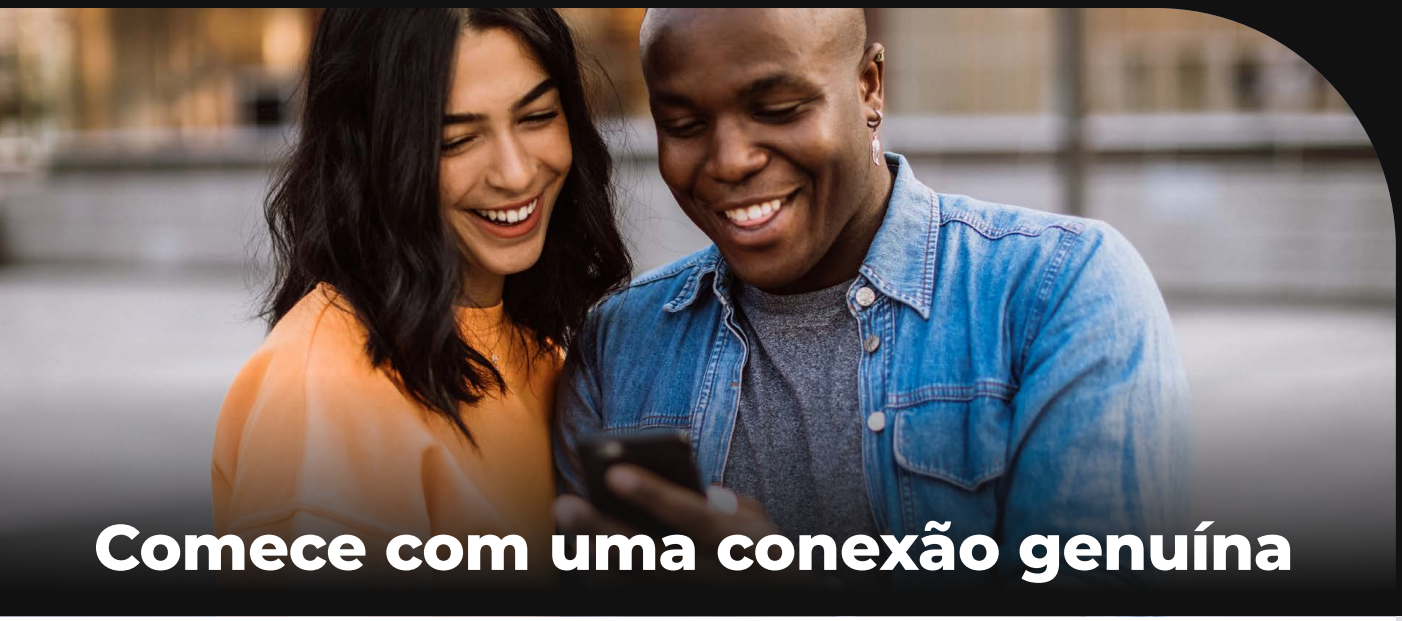
telesign

Fraude é um grande problema para as empresas com presença digital. Do onboarding às transações e todas as etapas intermediárias, sempre que um cliente faz login, há uma oportunidade para criminosos atacarem.

Felizmente, tecnologias como a autenticação multifator – uma criação da Telesign – estabelecem novos padrões na criação de contas e autenticação de identidade digital, cruciais para empresas que fazem negócios online.

Proteja sua empresa, a experiência do seu cliente – e seus resultados – contra agentes mal-intencionados.

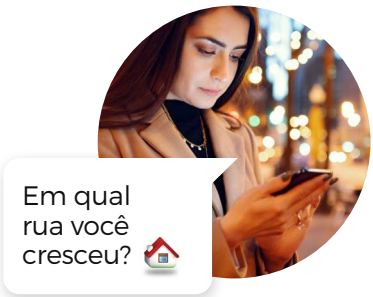




Comece com uma conexão genuína

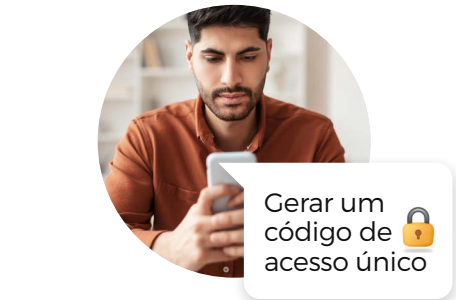
A confiança começa na primeira etapa da jornada do cliente. Offline é mais fácil—nas interações face a face, há dicas visuais que informam se você pode confiar na outra pessoa. Mas online seus invasores são invisíveis. Esse anonimato requer camadas adicionais de verificação. No entanto, pedir muitas informações pode afastar clientes reais em potencial. Qual é o ponto de equilíbrio?

Os blocos de construção da autenticação multifator



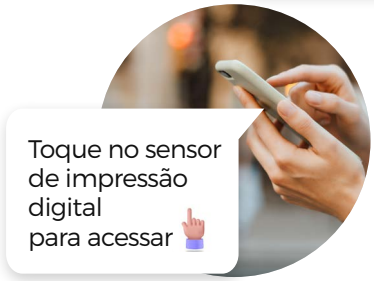
Algo que você sabe

Isso inclui identificadores baseados em conhecimento, como perguntas ou senhas que apenas uma pessoa real saberia.



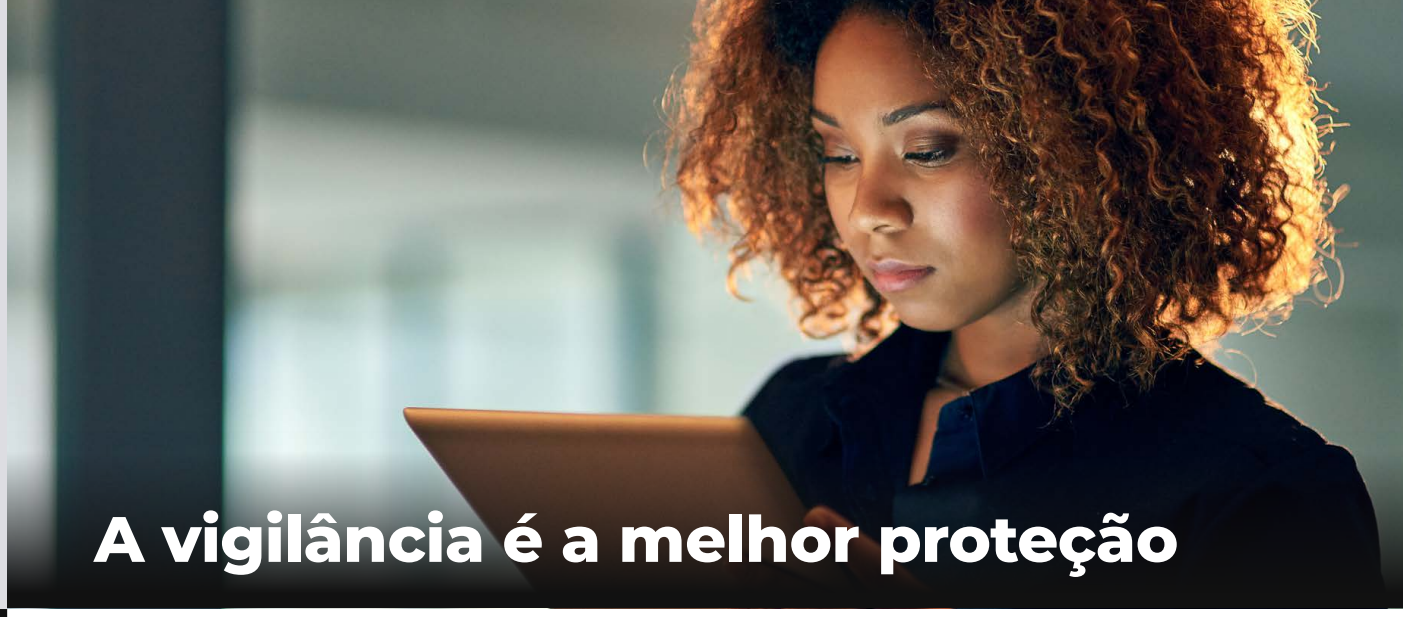
Algo que você tem

Isso inclui um token como um aplicativo autenticador que fornecerá uma nova senha sempre que o acesso seja necessário.



Algo que você é

Métodos biométricos e comportamentais estão se tornando cada vez mais comuns para empresas, como bancos.



A vigilância é a melhor proteção

Depois de verificar seus clientes, você deve mantê-los seguros sempre que eles se conectarem. Conhecer as diferentes maneiras pelas quais a jornada do cliente pode ser comprometida vai capacitá-lo a tomar medidas para manter a integridade de cada interação.

Tipos de métodos de controle de conta

Ataques de phishing

Os ladrões cibernéticos muitas vezes tentam se passar por marcas legítimas. Basta um clique para instalar um código malicioso que pode comprometer toda a organização.

Trocas de SIM

Usando informações geralmente coletadas de phishing, fraudadores convencem a operadora de celular da vítima a atualizar seu SIM para um novo dispositivo, burlando os protocolos de autenticação de dois fatores.

Senhas comprometidas

A maneira mais comum para os atores maus ganharem o controle é muitas vezes auto-infligida. A reutilização de senhas as torna suscetíveis a golpes e pode levar a roubo de identidades e transações fraudulentas.

Construa confiança em todos os canais

Autenticar a identidade dos seus clientes é um bom começo. Continue ganhando lealdade comunicando-se proativamente em todos os pontos de contato. Seja uma notificação para verificar uma ação ou um alerta sobre uma atividade suspeita, cada engajamento cria confiança em sua marca.

Mantenha seguros os canais que seus clientes usam

Os clientes estão em todos os lugares

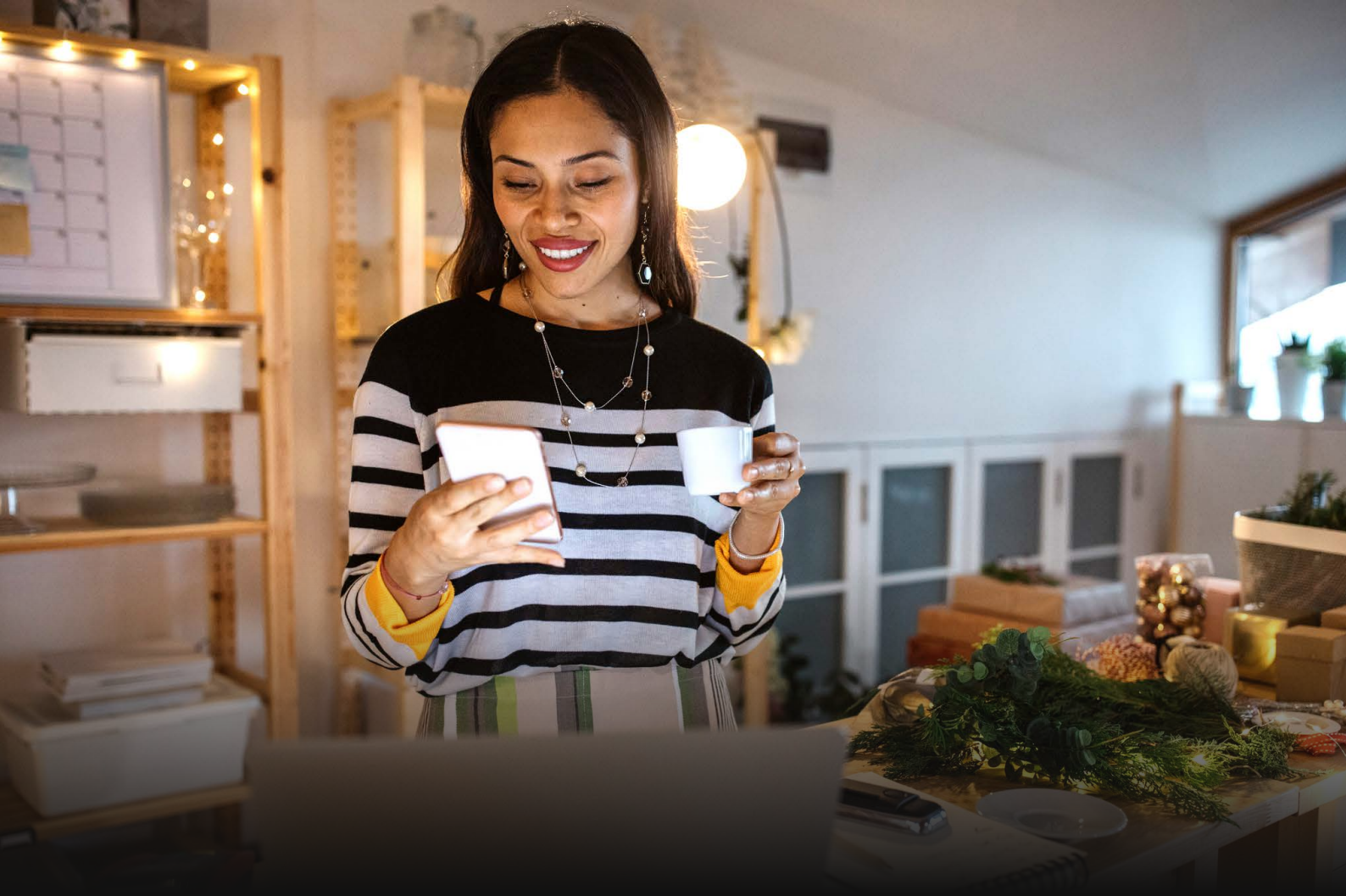
82% dos compradores B2B e 72% dos clientes B2C usam vários canais de comunicação ao longo do caminho até a compra[1].

Eles sabem do que eles gostam

Mais da metade dos clientes tem maior probabilidade de recomendar, comprar mais ou fazer uma primeira compra usando os canais de sua preferência[2].

Seja omnicanal para se conectar

Conecte-se e comunique-se nos canais que interessam a seus clientes, seja SMS, MMS, RCS ou WhatsApp.



Busque um especialista

Especialista em verificação e autenticação, a Telesign ajuda empresas de todos os tamanhos em todos os setores e regiões a criar confiança com seus clientes. Nosso conjunto de soluções de identidade digital reforça a jornada do cliente a cada passo para que seus clientes estejam seguros e sua empresa possa prosperar.

Porque quando você está protegido contra fraudes... o céu é o limite.

Referências

1 State of the Connected Customer. Salesforce.

2 What Businesses Need To Know About Communicating With Consumers. A Forrester Consulting Thought Leadership Paper Commissioned by Google. December 2020