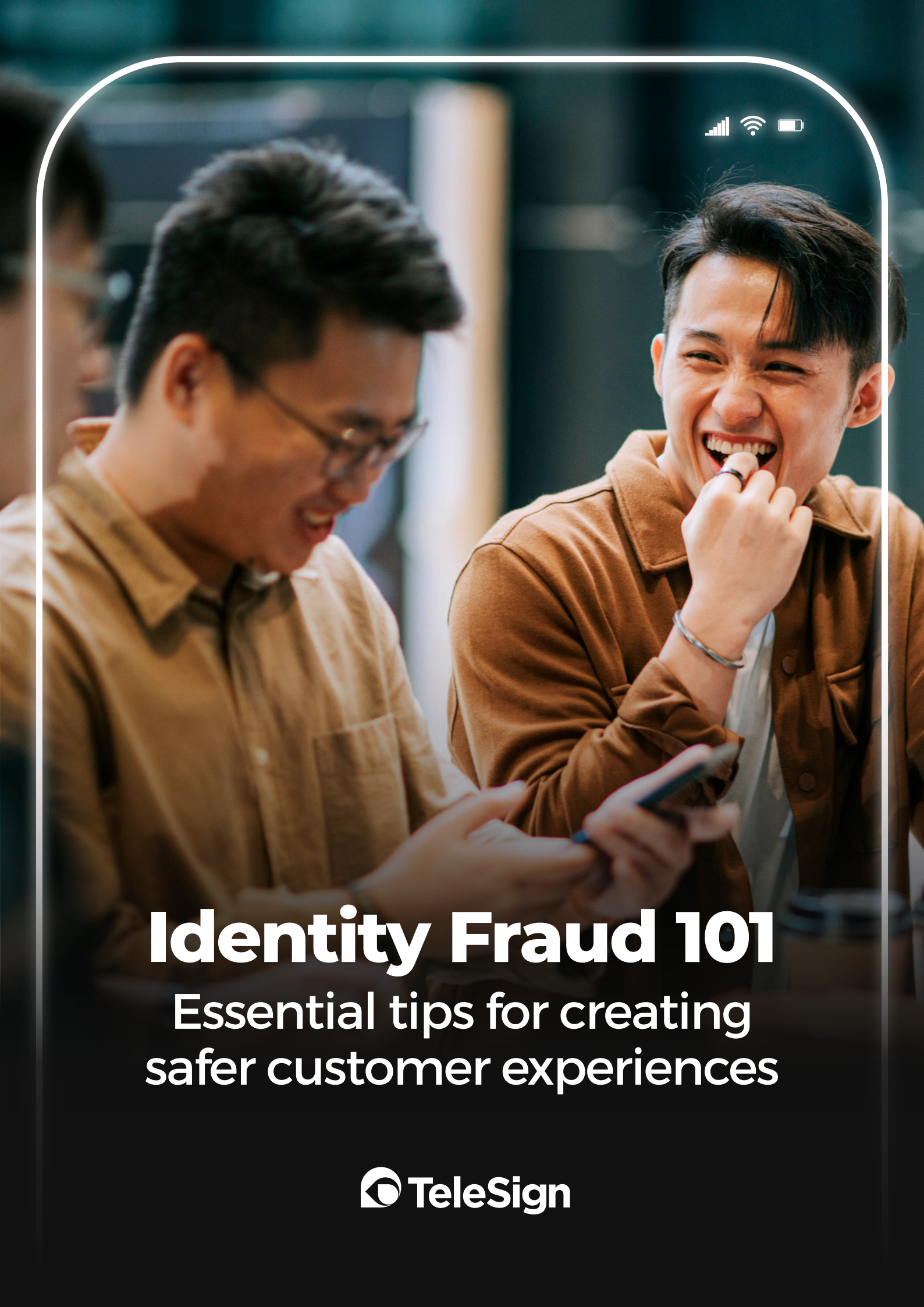


Identity Fraud 101

Essential tips for creating safer customer experiences

TeleSign

Fraud is a major problem for businesses with a digital presence. From onboarding to transaction and every engagement in between—every time a customer logs on, there's an opportunity for criminals to attack.

Thankfully, technologies like multifactor authentication—pioneered by TeleSign—set new standards in account creation and digital identity authentication, crucial for companies doing business online.

Protect your business, your customer experience—and your bottom line—from bad actors.

Start with a genuine connection

Trust begins at the first step of the customer journey. Offline, it's easier—in face-to-face interactions, there are visual cues that tell you if you can trust the other person. But online your attackers are invisible. This anonymity requires additional layers of verification. Yet asking for too much information can turn real potential customers off. What's the balance?

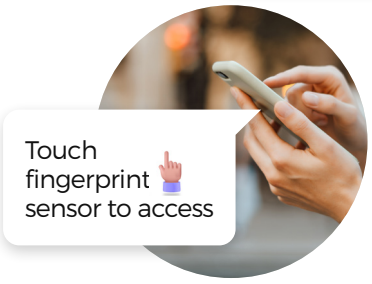
The building blocks of multifactor authentication

Something you know

These include knowledge-based identifiers such as questions or passwords that only real person would know.

Something you have

This includes a token such as an authenticator app that would provide a new password every time access is needed.



Something you are

Biometric and behavioral methods are becoming increasingly common for businesses, such as banks.

Vigilance is the best protection

Once you've verified your customer, you must keep them safe every time they engage. Knowing the different ways that your customer journey can be compromised can empower you to take action to maintain the integrity of every interaction.

Types of Account Takeover Methods

Phishing attacks

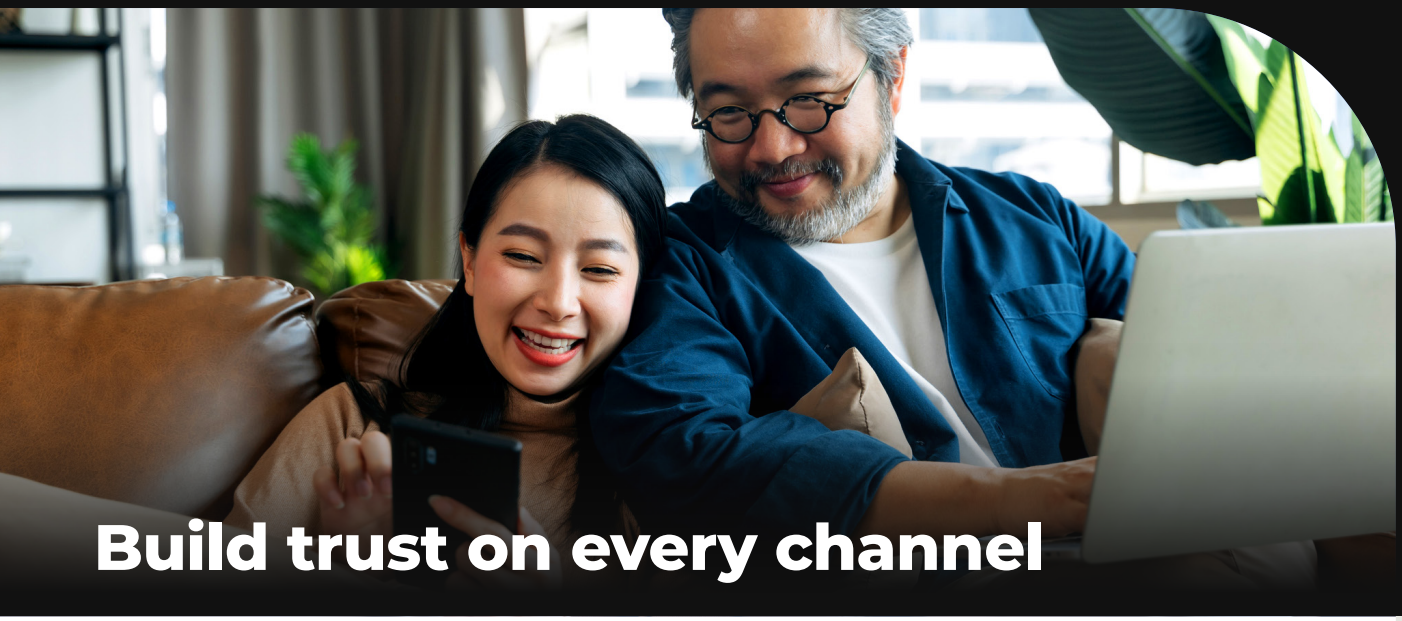
Cyber-thieves will often try masquerading as legitimate brands. All it takes is one click to install malicious code that can compromise an entire organization.

SIM swaps

Using information often gathered from phishing, fraudsters will convince a victim's mobile carrier to update their SIM to a new device, circumventing two-factor authentication protocols.

Compromised passwords

The most common way for bad actors to gain control is often self-inflicted. Reusing passwords makes them susceptible to theft and can lead to identity theft and fraudulent transactions.



Build trust on every channel

Authenticating your customers' identity is a good start. Continue to gain loyalty by pro-actively communicating at every touch point. Whether it's a notification to verify an action, or an alert about a suspicious activity—every engagement builds trust with your brand.

Keep the channels your customers use safe

Customers are everywhere

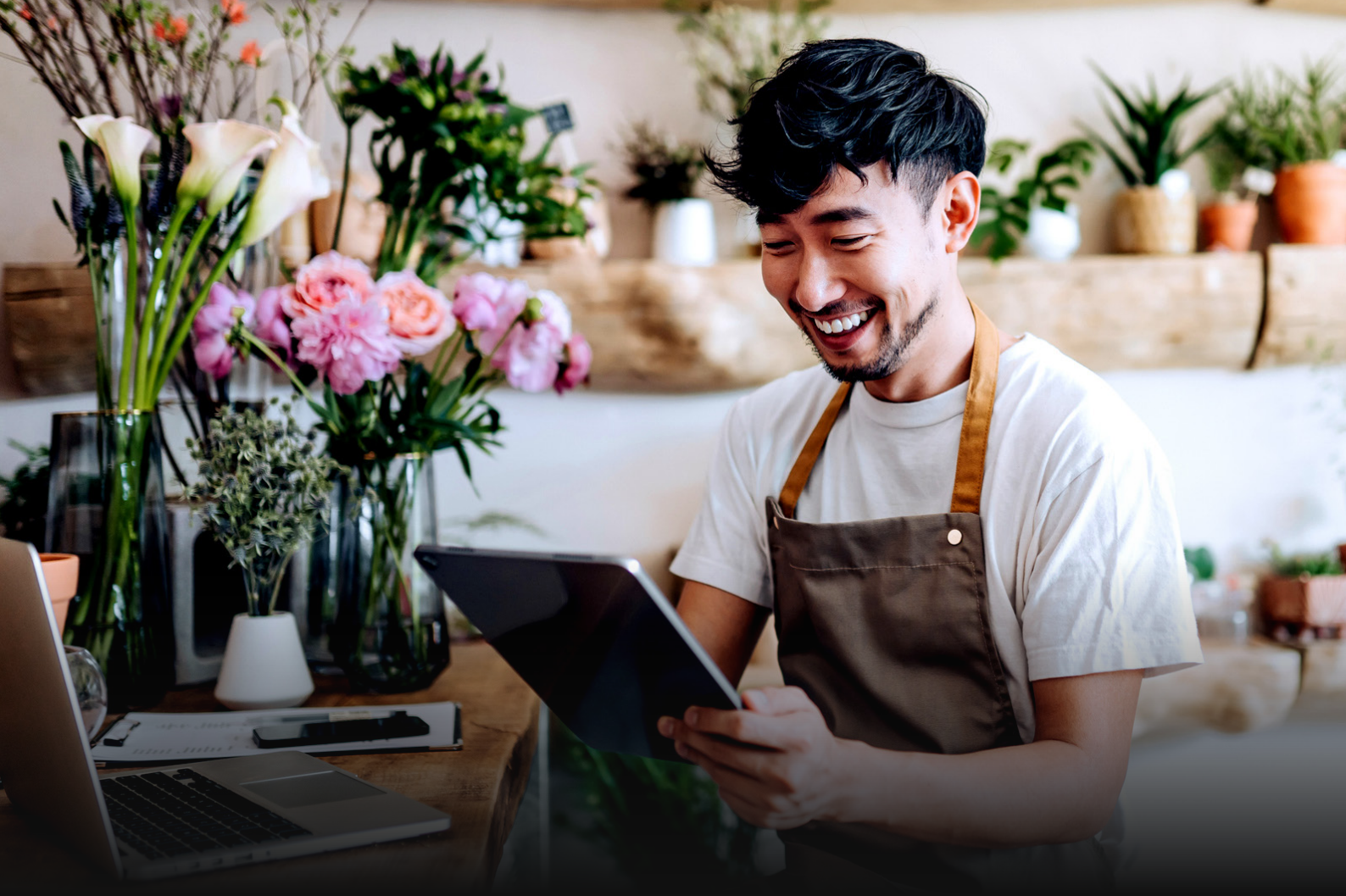
82% of B2B buyers and 72% of B2C customers use multiple communication channels throughout their path to purchase[1].

They know what they like

More than half of customers are more likely to recommend, buy more, or make a first-time purchase when using the channels they prefer[2].

Go omnichannel to connect

Connect and communicate on the channels that matter to your customers, whether it is SMS, MMS, RCS or WhatsApp.



Reach for an expert

Specialists in verification and authentication, TeleSign helps businesses of all sizes across every industry and geography to build trust with their customers. Our suite of digital identity solutions enhances the customer journey at every turn so your customers are safe and your business can thrive.

Because when you are protected against fraud... the sky is the limit.

References

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