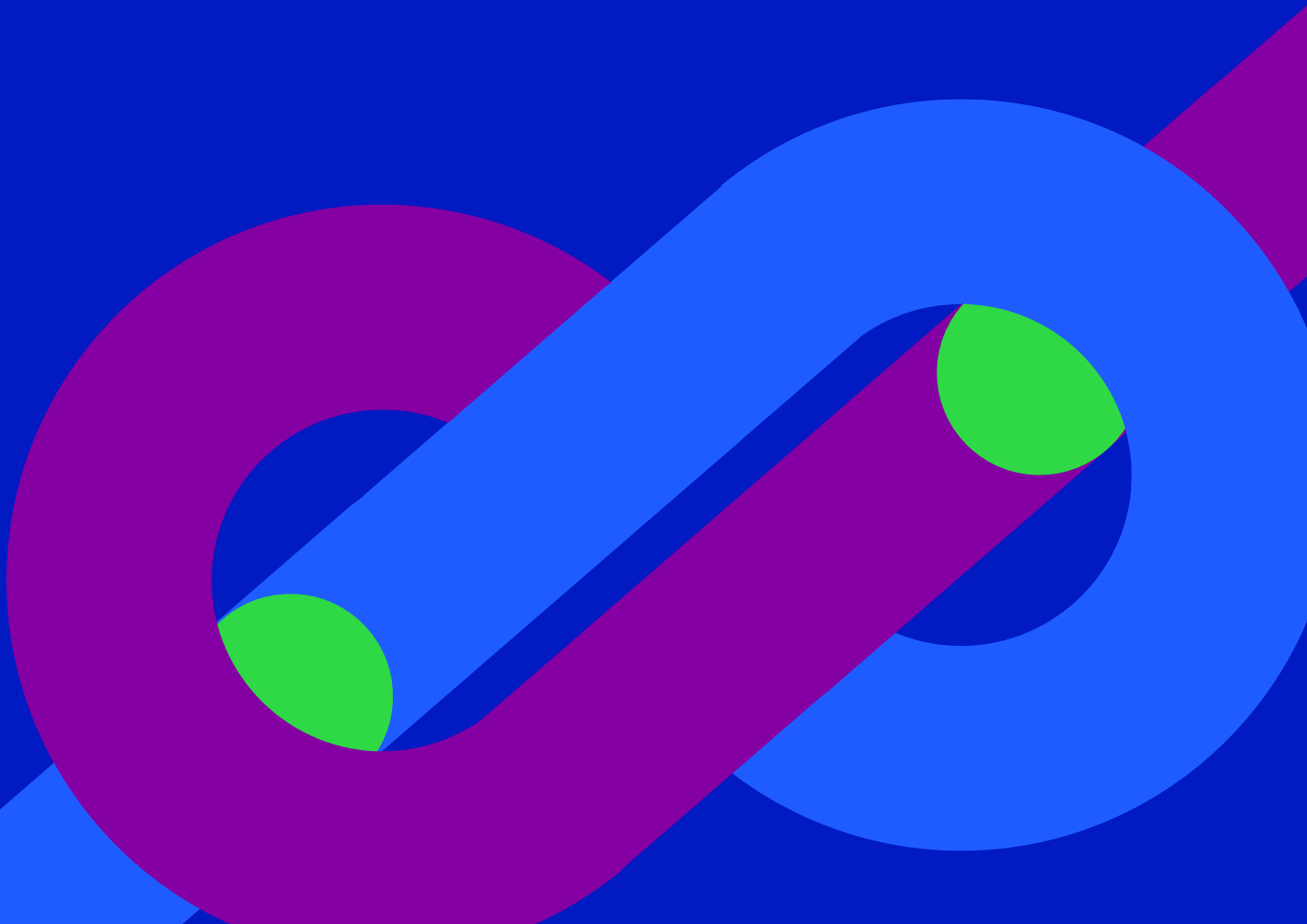# 2024 Telesign Trust Index

Trust in the AI era

What global leaders and businesses need to know about the critical role trust plays in the digital world amidst growing concerns over AI.

Trust matters, now more than ever.

The advent of generative AI has the potential to upend nearly every aspect of our lives. The 2024 Telesign Trust Index showcases how fear of the unknown is impacting consumer behaviors and perceptions, and the critical role trust plays in navigating the digital world.

Trust is foundational.

The second annual Telesign Trust Index reveals how the emergence of new technologies in the past year is magnifying the importance of trust globally across all levels of business and society. Public awareness of the potential impacts of artificial intelligence (AI) and machine learning (ML) remains murky, but with 7 of the 10 largest countries in the world set to head to the polls for elections in 2024, expect that to change in a big way as these emerging technologies dominate media headlines.

2024 Trust Index Key Findings

Business beware

Despite a massive increase in phishing and online fraud attempts following the rise of generative AI, most people remain surprisingly ambivalent about the impact it will have on their susceptibility to digital fraud. This could leave people vulnerable if the services they engage with online don't provide digital fraud protection. At the same time, an overwhelming majority of people believe brands they engage with are responsible for protecting them from fraud.

Fear of deepfakes

Most people do not believe that they have recently seen a deepfake video or voice clone online, yet the vast majority fear that misinformation from deepfakes and voice clones is negatively affecting their elections.

Trust in digital voting

Although a majority of people would prefer to vote online if they trusted the voting system, the reality is they don't trust the current systems and would question the outcome of an election held online.

AI-generated content increasing

Many people fear that AI-generated content will impact their elections, and nearly half of all people reported seeing an AI-generated political ad or message in the last year.

Fighting AI with AI

A majority of voters believe misinformation has made election results inherently less trustworthy. They also report that their trust in the outcome of the election would increase if AI or ML was used for good — such as to prevent or stop fraud, hacking and misinformation. While consumers appreciate 'AI for good' in the context of elections, there's a gap in their understanding of how the online services they use every day utilize AI and ML to protect them from digital fraud.

AI & FRAUD

In the U.S., 44% of respondents think AI/ML will have no difference on their susceptibility to digital fraud. Globally, the average is lower at 32%.

Nearly all Americans (87%) believe that the companies they engage with are responsible for protecting users' digital privacy.

US	**44%**
GLOBAL	**32%**

0% 10% 20% 30% 40% 50%
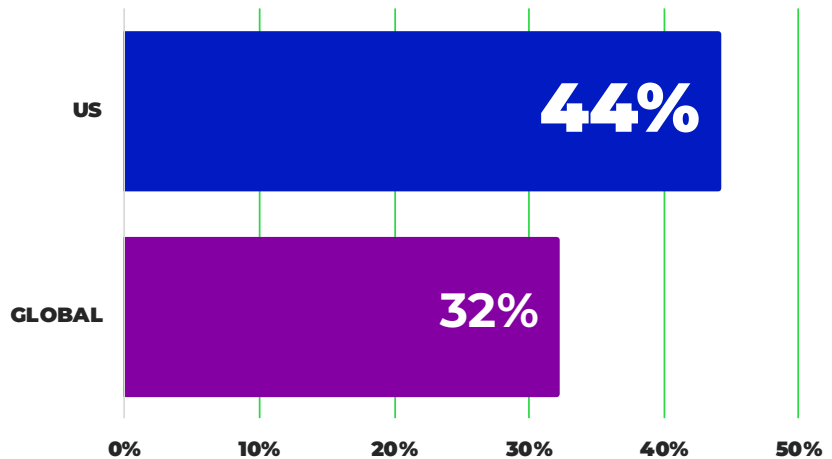
Only 34% of U.S. respondents are more likely to trust a company that uses AI or ML to protect them from fraud attacks. Globally, 43% are more likely.

Younger people are also more likely (47%) to trust companies that utilize AI or ML to protect against attacks than older people (39%) from fraud.
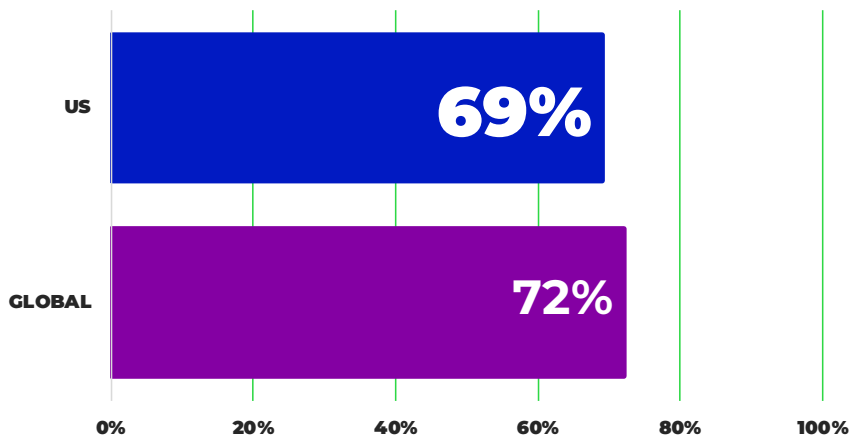
US	**34%**
GLOBAL	**43%**

0% 20% 40% 60% 80% 100%
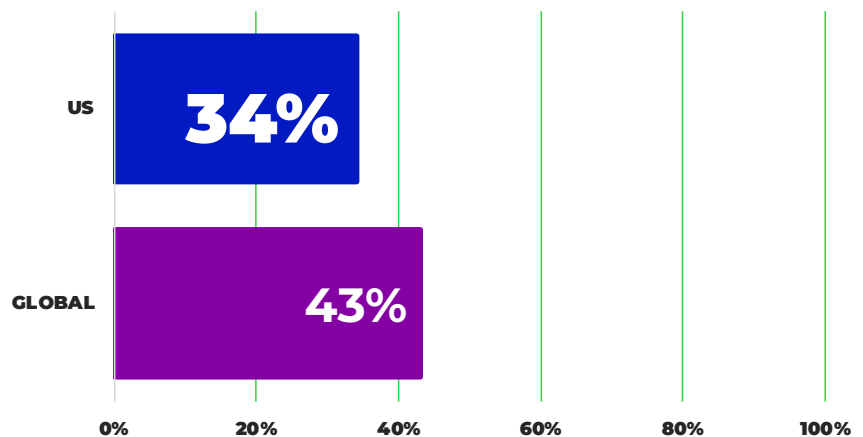
Notably, nearly twice as many Brazilians (63%) are more likely to trust a company that uses AI or ML to protect them from fraud attacks.
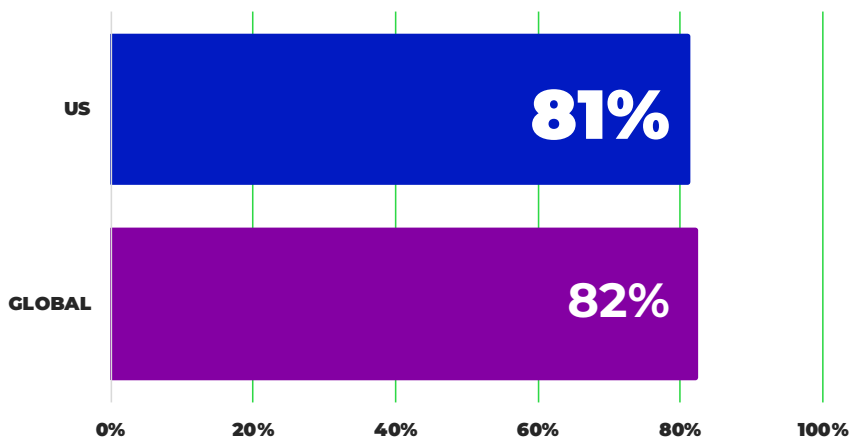
AI & DEEPFAKES

US 69%

GLOBAL 72%

0% 20% 40% 60% 80% 100%

69% of respondents in the U.S. do not believe that they have been recently exposed to deepfake videos or voice clones. Global average increases to 72%.

Fraud victims are **more likely to have been exposed to a deepfake** or clone in the past year (21%).

US 81%

GLOBAL 82%

0% 20% 40% 60% 80% 100%

The vast majority of Americans surveyed (81%) fear that misinformation from deepfakes and voice clones is negatively affecting the integrity of their elections. Global average is 82%.

People who identify as liberal (38%) and conservative (35%) **strongly agree that misinformation is negatively affecting elections** compared to those who identify as moderate (28%).
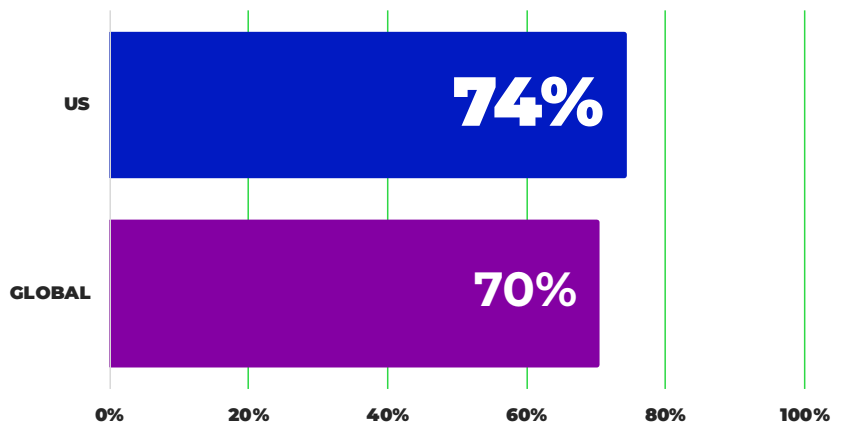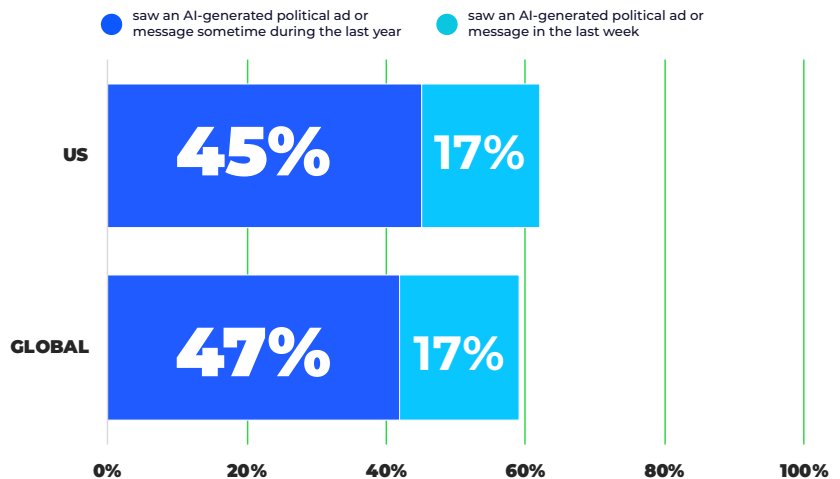
AI & ELECTIONS

In the U.S., 17% of respondents report seeing an AI-generated political ad or message in the last week, while 45% have seen one sometime during the last year. Globally, 17% report seeing an AI-generated political ad or message in the last week, while 47% of people have seen one in the last year.

Those aged 45+ are much more apt to be unsure (41%) of whether they have seen an AI-generated ad or message than those ages 18-44 (20%).

74% of U.S. respondents agree that they would question the outcome of an election held online. Global average is slightly lower at 70%. **Americans are the least likely to trust online election results.**

People who identify as conservative are more likely (76%) to question the outcome of an online election than those who identify as liberals (67%) and as moderate (70%).

● saw an AI-generated political ad or message sometime during the last year   ● saw an AI-generated political ad or message in the last week

US — 45% | 17%

GLOBAL — 47% | 17%

0%   20%   40%   60%   80%   100%

US — 74%

GLOBAL — 70%

0%   20%   40%   60%   80%   100%

At the same time, 62% of Americans would prefer to vote online if they trusted online voting systems. Globally, that number increases to 69%, with Americans showing the least amount of enthusiasm for online voting. Brazilians and Singaporeans (74%) registered the strongest preference for online voting.
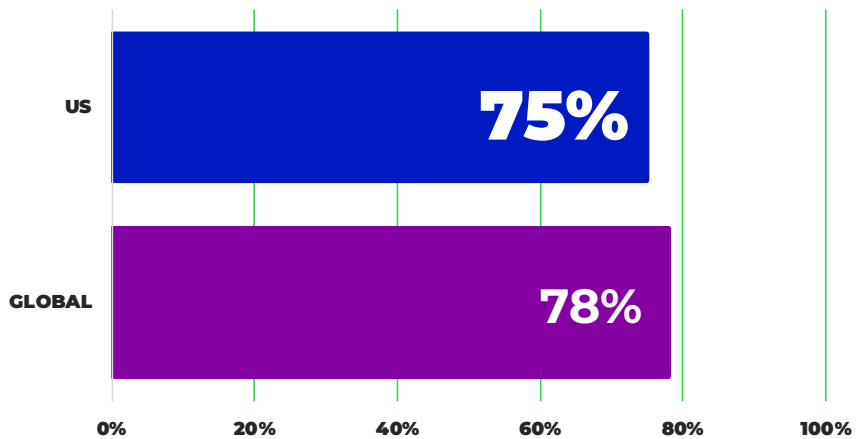
AI & ELECTIONS

A large majority of American respondents (71%) are more likely to trust the outcome of an election if AI and ML is used to prevent cyberattacks, voter fraud, and hacking. Global average is higher at 76%.

Meanwhile, 83% of Brazilians would be more likely to **trust the outcome of an election if AI and ML is used to prevent cyberattacks, voter fraud, and hacking.**

US 71%

GLOBAL 76%

0%   20%   40%   60%   80%   100%
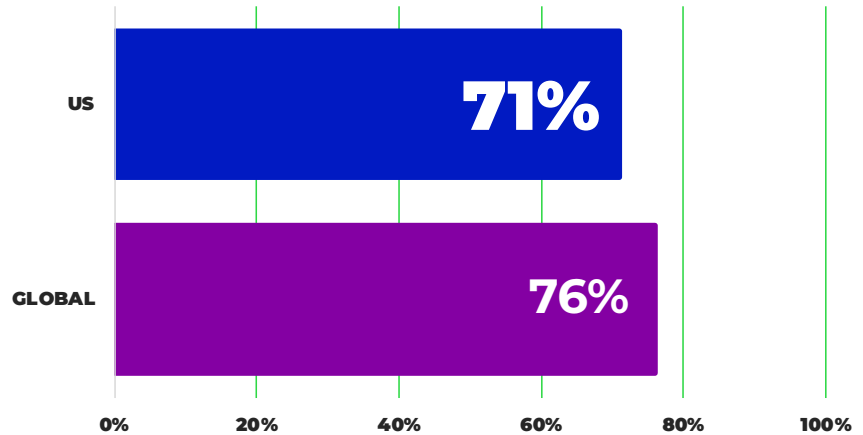
In the U.S., three out of four (75%) people believe misinformation has made election results inherently less trustworthy. Global average is 78%.

Along the same lines, roughly three-quarters (73%) of Americans **fear AI-generated content will undermine upcoming elections,** in line with the global average (72%).

US 75%

GLOBAL 78%

0%   20%   40%   60%   80%   100%

Conservatives are more likely to agree (82%) that misinformation has made election results less trustworthy compared to people who identify as liberals (72%).

Key insight for businesses

Digital technologies are transforming our world faster than businesses have been able to transform their digital infrastructure.

The COVID-19 pandemic accelerated this transformation years ahead of what most experts thought was possible. The debut of ChatGPT and the subsequent surge in AI development has accelerated the pace of innovation at an even greater rate.

Many businesses have been quick to recognize the potential economic benefits of integrating AI into their digital infrastructure. According to data from CompTIA, a leading voice for the global IT ecosystem, 55% of firms are already engaging in at least a limited implementation of AI.

For all the promise AI holds, it also brings significant challenges. Fraudsters have discovered that AI tools can be used to streamline fraud and cyberattacks, leading to more than a 1,000% increase in phishing since the launch of ChatGPT.

As the volume of digital business rises year over year, the potential for AI-enhanced digital fraud increases with it. The good news: businesses are taking note. Forbes Advisor reports that 51% of businesses are using AI to help with cybersecurity and fraud management. In the near future, every business will need to fight AI with AI.

The second annual Trust Index examines the pivotal role trust plays in a world shaped by the emergence of generative AI. The findings offer insights into consumer sentiment toward AI and ML, and the resulting shifts in how people engage with businesses and services online, the content they see on social media and even how they vote.

The study revealed a dichotomy of desires, with consumers wanting AI's protection against existential threats to democracy and elections yet remaining ambivalent about its ability to safeguard their personal data from digital threats.

Fear of the unknown also emerged as a common theme, presenting an opportunity for businesses to not only embrace AI and ML technologies but also to showcase their commitment to safeguarding customer data. In the era of AI, businesses stand at a crossroads, tasked with not only adopting innovative technologies but also fostering trust. Those who navigate this challenge successfully will emerge as beacons of trust in the digital world.

What are the latest digital fraud trends businesses should be aware of?

Digital fraud tactics evolve quickly, making it essential for companies to stay up to date on the most prevalent trends and prevention strategies in order to build and keep customer trust. The latest tactics fraudsters are using to steal from businesses and their customers include:

Account Takeovers

Generative AI has enabled fraudsters to super-charge phishing attacks. Data from the **12-month period following the launch of ChatGPT showed a 1265% increase in malicious phishing messages and a 967% increase in credential phishing.** Gone are the grammar and translation errors of pre-AI phishing messages. With the help of generative AI, fraudsters can easily correct these mistakes resulting in more convincing and harder to spot phishing attempts. And they're using them to steal credentials, takeover accounts, infiltrate companies and steal customer data. It's critical for businesses to use technology to detect signs of account takeovers to stop them in their tracks.

Exploiting MFA

Multi-factor authentication (MFA) was **inactive in approximately 99% of successful digital intrusions,** according to data from Microsoft. While MFA has been around for a long time, many companies are still not using it consistently. The solution is simple, MFA needs to be turned on by default to protect the digital infrastructure of every business. Proper training of IT staff and the rest of the enterprise is also critical for staving off social engineering intrusions that take advantage of gaps in MFA.

Fake Accounts

The proliferation of fake accounts also poses a significant threat to companies operating online. Individuals sneak their way into online communities by creating fake accounts, wreaking havoc among legitimate users and ultimately tarnishing brand reputations. A growing challenge closely associated with the use of fake accounts is the emergence of deepfakes or voice clones.

While technology firms are making strides in how to quickly identify, label, and remove AI-generated images and videos from the digital world, not enough attention is paid to how this content is distributed. One of the primary ways is through fake accounts, online and via social media. The best way for businesses to stop the spread of fake accounts is by improving their Know Your Customer (KYC) processes to raise the bar in proving users are real.

Methodology

This survey was fielded online and reached a total of n=1,000 completions in each market. Those surveyed were adults across the United States, United Kingdom, Singapore, and Brazil aged 18+; a subset of which have been victims of digital fraud within the past three years.

The survey was fielded between March 11 – April 6, 2024. The margin of error is +/- 3.1 percentage points for each market.

About Telesign

Telesign provides Continuous Trust™ to leading global enterprises by connecting, protecting, and defending their digital identities. Telesign verifies over five billion unique phone numbers a month, representing half of the world's mobile users, and provides insights into the remaining billions. The company's powerful machine learning and extensive data science deliver identity risk recommendations with a unique combination of speed, accuracy, and global reach. Telesign solutions provide fraud protection, secure communications, and enable the digital economy by helping companies and customers to engage with confidence. Learn more at www.telesign.com and follow us on X, formerly known as Twitter, at @Telesign.