



STATE OF THE CALL 2025



262.8 billion calls analyzed
1.8K+ businesses surveyed
12K+ consumers surveyed
600+ carrier decision-makers surveyed

hiya.com/state-of-the-call

State of the Call 2025

For consumers and businesses alike, voice communication remains absolutely critical. In fact, the number of consumers and businesses who say that voice calls are essential, especially in situations involving sensitive information, has only increased in recent years. Even in an increasingly digital world, people crave the human connection that voice provides.

Yet at the same time, individuals and businesses report persistent struggles in making calls reliably and securely:

- Individuals worry about their ability to trust voice communication in an era of rampant spam and fraud calls.
- For businesses, reaching consumers by phone is increasingly difficult as scammers impersonate brands, damaging trust and deliverability. At the same time, organizations themselves are frequent targets of attacks, from voice-phishing to social engineering.

These challenges reflect long-standing voice security and trust issues, such as spam and fraud calls. However, they have been exacerbated over the past year by newer, more sophisticated threats, such as AI-powered deepfakes that are harder to detect than conventional phone scam techniques.

80%

of unidentified calls are likely to never be answered.

The result is much more than mere annoyance or inconvenience. Consumers and businesses are losing money when they fall victim to voice scams, or when they feel they can no longer rely on voice calls for secure and effective communication.

The good news: AI-powered solutions already exist to tackle many of these challenges, improving the phone experience by boosting both security and productivity.

Unfortunately, although some consumers and businesses are actively seeking out and leveraging technologies like these, not all are taking full advantage of the latest

innovations to improve the call experience. This has led to a gap between what the voice calling experience should be and what it too often becomes in practice.

This year's State of the Call Report is based on Hiya's analysis of more than 262.8 billion calls, as well as survey responses from more than 12,000 consumers, 1,800 workers who use voice calls on the job and 600 security and IT executives at businesses that depend on voice calls. It highlights five major trends that impact the voice call experience in 2025. It also showcases current efforts—and future opportunities—to improve the call experience for all stakeholders.

Understanding unwanted calls

At Hiya, we use the term “unwanted call” to refer to a voice call that originates from outside a recipient’s contact list that consumers don’t want to receive. Unwanted calls range from illegal fraud attempts to steal money or personal data, to legal but irritating nuisance calls that frustrate consumers.

Unwanted calls are sometimes labeled as spam or fraud on consumers’ mobile devices. However, many of the calls that consumers deem unwanted are not labeled at all. Nearly half—48 percent—never answer unidentified calls, and another third—33 percent—rarely answer them. This means a whopping 80 percent of unidentified calls are likely to never be answered.

In the case of the other half of unidentified calls—those that consumers do pick up—recipients typically only

answer reluctantly, due to concerns that it may be a call they can’t miss. Only 20 percent of consumers report that they always answer unidentified calls.

Hiya tracks unwanted call metrics by analyzing calls placed by parties outside an individual’s contact list. Based on a variety of data points, we assess when calls are unwanted, then block or label calls accordingly. We also monitor how consumers respond to unwanted calls, and we track unwanted call data across a number of carrier networks and regions.

The insights in this report reflect our ongoing analysis of unwanted call trends. They highlight how the latest unwanted call data compares to trends from previous years, while also presenting survey findings and insights from consumers, enterprises and IT and security executives.



Top voice call trends from 2025

Key findings from this year's State of the Call Survey:

1

Voice remains a critical communication medium for consumers and businesses alike. Across most types of communication categories, use of voice calls remained the same or increased from previous years. Businesses also increased investment in voice calling technology; for example, 40 percent of businesses are looking to add a branded calling solution in 2025 to gain advantage over their competitors.

2

Consumers, employees and IT professionals express significant concern about the security and reliability of voice calls. Spam calls, unknown caller IDs, and voice scams create major challenges—prompting 60 percent of IT departments to plan call protection investments in 2025.

3

Alongside traditional voice spam and scam threats, deepfakes have emerged as a novel challenge that further threatens voice. Deepfake calls that convincingly mimic the voice of someone known to a target have become easy for attackers to generate using AI tools. 39 percent of consumers and nearly half of employees report having been impacted by a deepfake attack in just a single recent three-month period.

4

Voice calling challenges have a serious financial impact on consumers and businesses. 15 percent of consumers say they lost money to a phone scam in 2024, and about one-third of workers report that voice calling challenges cost their business money.

5

While some businesses are investing in call protection, many aren't fully leveraging it. Only a third of employees use personal spam detection apps—often self-installed. And most companies adopt call confirmation tech only after falling victim to a scam.

The report dives into each of these trends, while also touching on other items of note—such as the struggles IT departments face in securing voice communications and protecting their own users against scams, especially when many of the devices that employees use for voice calls are not owned or directly managed by the company.

The criticality of voice calls

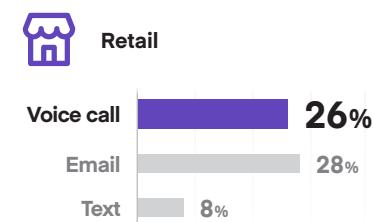
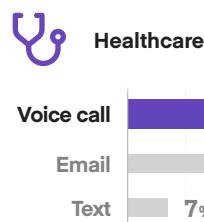
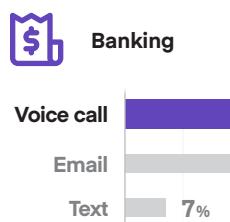
Texting and emails may be a popular way for consumers to communicate with friends and for businesses to send automated messages to customers. But State of the Call survey data makes clear that when the stakes are high, people turn to voice calls.

In domains like finance and healthcare, where communication often requires sharing private information, the strong majority of consumers report that voice is their preferred

communication medium. Even for communicating with retail businesses, where data tends not to be so sensitive, three times as many consumers prefer voice as compared to text.

Also notable is that in certain domains, the percentage of consumers who prefer voice calls has increased. For example, when communicating with healthcare providers, 42 percent of consumers said they prefer voice in 2025 compared to 33 percent in 2024.

Consumer communication preferences



The trend surrounding voice as the go-to communication channel also holds true when it comes to the ways businesses engage their customers. A majority of workers consistently reported that they turn to voice for critical needs, like resolving customer issues and closing sales.

The preference for voice has increased in some areas over the last year. For instance, this year's State of the Call report found that 30 percent of workers preferred voice for closing

sales, compared to 27 percent in last year's report.

Overall, 29 percent of workers said that they had increased their use

of voice communications on the job over the past year, while 57 percent said it had stayed the same. Only 11 percent reported that they are relying less on voice today than a year ago.

Working professionals report their top uses for voice calls are:

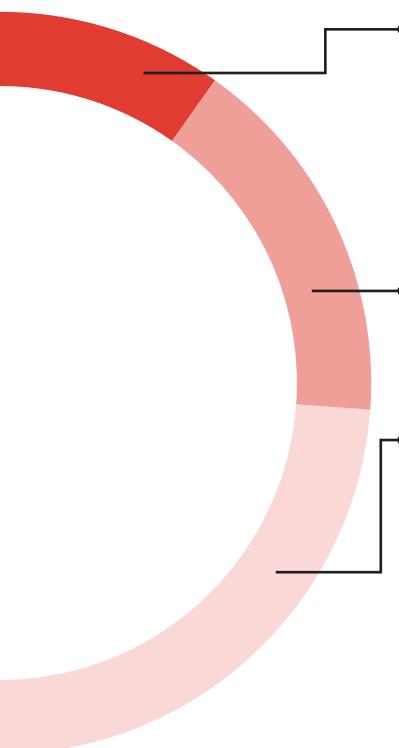
Business need	Voice	Email
Resolving customer issues	39%	31%
Closing Sales	30%	26%

Persistent concerns about voice security

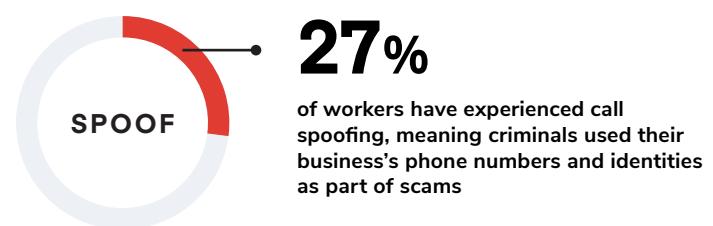
While consumers and businesses continue to rely heavily on voice communications, many struggle to take advantage of voice as seamlessly as they would like.

For consumers, the main challenge is unwanted calls—such as spam, fraud, and any other voice messages they didn't ask for or don't want. A majority of consumers report receiving 8 unwanted calls per week. This represents an increase from 2024, when the average consumer received 4.8 unwanted calls weekly. Consumers also report that phone spam is getting worse, with a majority indicating that they have received “a lot more” spam calls in the past twelve months.

The challenges consumers face surrounding voice security center in large part on unidentified calls:



This trend dovetails with a challenge reported by businesses in the survey, which often struggle to reach customers because employees' outbound calls are delivered in ways that make consumers less likely to answer:



Call spoofing risks present an especially acute challenge for IT security professionals. 93 percent say they are concerned about bad actors impersonating their business to scam consumers.

The bottom line: Consumers and businesses want to use voice, but they often feel that they cannot trust it.

The surging deepfake threat

Scammers have long used methods like number spoofing and robocalls to increase their ability to reach targets. Even as those threats persist, bad actors are also turning to a new, more insidious technique:

Deepfakes.

A deepfake uses AI to convincingly mimic someone's voice or image. In voice calls, this allows attackers to sound like someone the recipient knows and trusts.

Survey data shows deepfakes are becoming alarmingly common—echoing FBI findings that [40 percent](#) of online scams in 2023 involved deepfaked content and Department of Homeland Security [warnings](#) that their use will rise as creation becomes cheaper and easier.

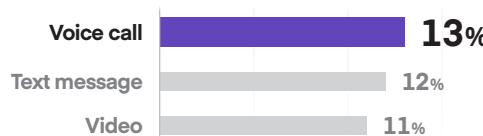
During a three-month period starting in late 2024, 39 percent of consumers reported experiencing a deepfake communication. While social media channels are the most common environment where deepfakes arise, voice calls are a popular attack medium, too.

Where workers encounter deepfakes most often



The impact of deepfakes goes beyond financial loss—attackers use them in phishing and social engineering to steal employee credentials. That's why 94 percent of IT leaders are concerned about AI-generated deepfakes, and over half are “very concerned.” While 70 percent say their companies have invested in detection tools or training, nearly 40 percent still lack strong confidence in their ability to fully mitigate the threat.

Where consumers encounter deepfakes most often

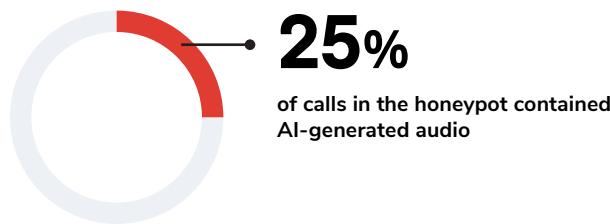


The deepfake scourge is not limited to consumers. In the same three-month period mentioned above, about half of workers experienced a deepfake of some type, with audio or voice communications near the top of the list of deepfake types.

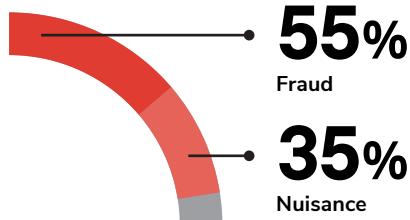
The surging deepfake threat

1 in 4 spam calls in the U.S. now use AI-generated voices

In Q1 2025, between January 10 and March 20, Hiya's Audio Intelligence team used [Hiya's AI Voice Detection](#) product to run thousands of spam call recordings through its audio deepfake detector. They ultimately captured 8,455 calls with sufficient speech for analysis. The result:



Using a subset of the AI-generated calls, the team conducted a deeper analysis to identify the intent behind each one, finding:



Of the calls that were AI-generated, 55% were identified as fraud — scams that used audio deepfakes to deceive recipients — while 35% were classified as nuisance, annoying perhaps, but legal and relatively harmless. The intent of the remainder could not be determined or were mistaken calls to wrong numbers.

The data reveals a troubling new trend: the rise of deepfake scams. Calls using AI-generated voices are significantly more likely to be fraudulent, with bad actors leveraging synthetic audio to deceive and exploit people. While AI tools are accessible to both good and bad actors, we're now seeing AI-generated voices in many fraud and nuisance calls.

Here are just a few examples of AI-generated scam calls captured in the Hiya honeypot in Q1:

- | [Google business listing scam](#)
- | [Cable TV discount scam](#)
- | [Debt management scam](#)
- | [Tax relief scam](#)

The financial fallout of calling challenges

15%

of consumers say they lost money to a phone scam in the last year

33%

of workers say their company has lost money because they couldn't reach customers by phone.

33%

of people say they are considering switching services due to how their mobile carrier handles spam and fraud calls.

Sometimes, unwanted calls are merely annoying or a waste of time. But too often, they result in significant financial losses for consumers, businesses and mobile carriers.

Consumers

Phone scams continue to result in significant financial losses for consumers. Over the past year, 15 percent of consumers reported losing money to a phone scam—a figure that remains virtually unchanged from 2024, despite ongoing investments by carriers and device manufacturers in voice security.

Among those who lost money, the average amount reported over the past 12 months varied by country:



United States

\$539
lost



United Kingdom

£595
lost



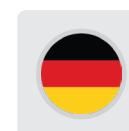
Canada

\$1,479
lost



France

€1,089
lost



Germany

€723
lost



Spain

€556
lost

The financial fallout of calling challenges

Businesses

For businesses, the financial and operational cost of spam and fraud calls is even steeper.

Roughly one-third of workers say their company has lost money because they couldn't reach customers or prospects by phone. The impact is especially acute in sales—60 percent of sales professionals report losing a deal due to call-related issues.

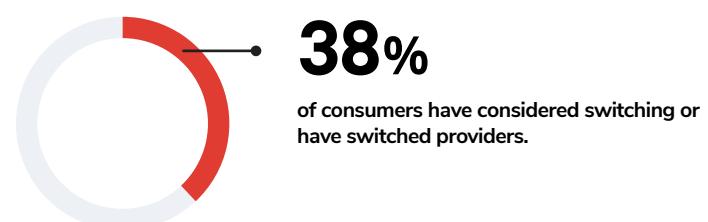
But the damage goes beyond lost revenue. Business professionals report a wide range of negative consequences from not being able to reliably reach customers by phone, including:



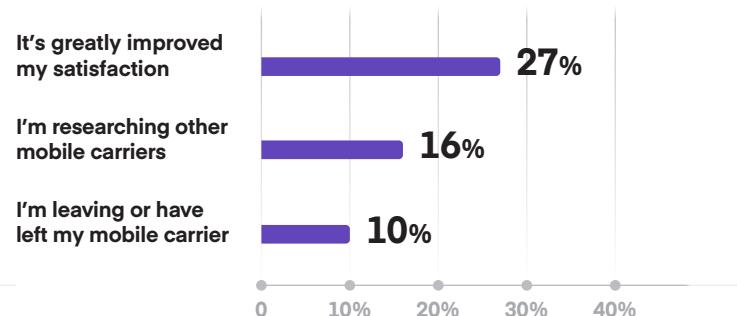
Mobile Carriers

Switching Providers: The Impact of Spam and Fraud on Customer Loyalty

We asked consumers whether spam and fraud calls had ever made them consider switching mobile providers. The results show a clear link between voice security and customer retention: more than one-third of consumers say they have either switched providers or considered doing so due to how their current carrier handles spam and fraud calls.



Beyond switching behavior, spam and fraud call management has a measurable impact on customer satisfaction. Just over half of consumers said that how well their mobile carrier handles these issues has either positively or negatively affected their satisfaction.



Under-investment in call protection solutions

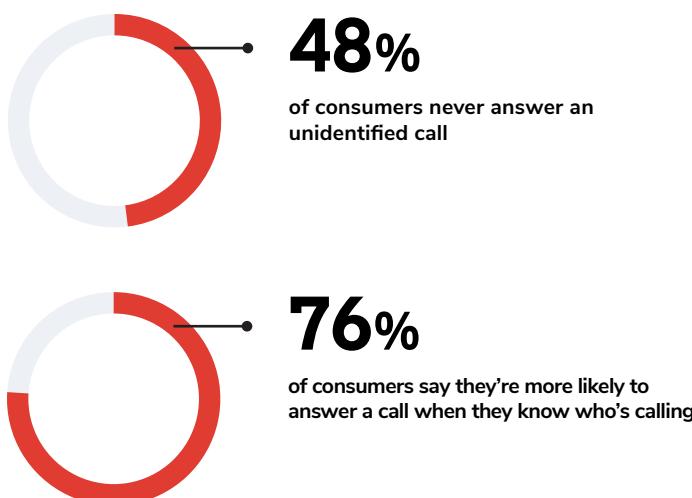
Consumers and businesses face many challenges when it comes to call security, but solutions are available.

For consumers, call protection apps can block unwanted calls. They can also help identify those that involve spoofing or fraud. Advanced call protection apps can even detect deepfakes. However, two-thirds of consumers reported using no call protection apps—a missed opportunity to help keep voice calls secure.

As for businesses, several approaches can help improve the effectiveness of voice:

- Registering as a legitimate business with mobile carriers.
- Identifying the business to call recipients by displaying caller identity.
- Coaching agents on best calling practices.

Measures like these are likely to improve call answer rates for businesses because call identification correlates closely with improving consumer trust and answer rates:



Call improvement technique	Most effective
Add business identity to calls	30%
Ensure calls don't have a spam label	19%
Increase agent coaching	12%

From the perspective of IT leaders, too, technologies that improve call deliverability through measures like branded calling and spoof protection are valuable ways to enhance the security and reliability of voice—and some say their businesses are already using measure like these to help prevent impersonation of their business by phone scammers:

Anti-impersonation technique	Adoption rate
Customer education about fraud risks	61%
Call confirmations (via email or application)	57%
Spoof protection service or tools	56%
Branded calling	49%

When it comes to anti-deepfake solutions, too, 74 percent of businesses report investing in protections of various types:

Anti-deepfake technique	Adoption rate
AI-powered detection tools	71%
Enhanced security policies	69%
Employee training and awareness programs	67%
Collaboration with third-party experts	52%

Deployment of anti-deepfake technologies is encouraging given the growing prevalence of this threat.

SPOTLIGHT

The BYOD challenge

When it comes to protecting workers from voice-based scams, businesses face another layer of difficulty due to the prevalence of Bring Your Own Device (BYOD) policies, which allow employees to use personal devices at work. Because businesses don't control those devices directly, they can't always deploy the full set of voice security solutions that they run on company-owned phones.

But they can—and do—take other measures to secure BYOD devices.

BYOD protection technique	Adoption rate
Multi factor authentication processes	65%
Required employee security training	63%
Regular education and communication to employees	57%
Inbound anti-fraud authentication tools	56%
We are not taking any measures	1%

In our survey, IT leaders reported that about 68% of businesses have a BYOD policy that covers employee smartphones. While many organizations have taken steps to secure these personal devices, only around half have implemented inbound anti-fraud authentication—a critical technique that helps verify incoming voice calls and protect employees from impersonation attacks. But for the just shy of half without it, a BYOD program may unintentionally open the door to deepfake phishing and social engineering attacks, especially when employees can't spot a scam based on training alone.

With the rise of deepfake voice scams and BYOD policies, securing employee communications is more critical than ever. Solutions like [Hiya AI Phone](#) helps safeguard employees from voice-based fraud and social engineering attacks—while boosting productivity through smart call screening and prioritization.

Even better: the technology behind the Hiya AI Phone is available to Hiya partners to integrate into their own apps, devices, or network-based services—ensuring flexible, scalable protection across any environment.

Recommendations

Given the critical role that voice calls play in facilitating both personal and business communication, what can consumers and companies do to help keep voice channels secure and reliable?

Improving call security and reliability for consumers

Consumers can take steps to mitigate risks linked to voice calling through practices such as:

- Installing call protection apps, which can gather caller identity while also detecting spam, fraud and even deepfakes.
- Choose a mobile carrier or phone manufacturer with strong spam and fraud call protection. Look for providers that are highly rated for their voice security features, such as real-time spam detection, call labeling, and AI-powered fraud prevention.
- Reporting unwanted calls to mobile carriers via built-in tools or third-party apps.

Protecting voice calling for businesses

For businesses, protecting the integrity of the voice channel and safeguarding customers from call fraud requires proactive measures. Good practices include the following:

Business number registration

Businesses can [register their phone numbers](#), which establishes them as a legitimate caller to mobile carriers that deliver their calls. While this practice doesn't guarantee that a number will never be labeled as spam, it can help reduce the risk. It's an important—and free—step that every business making outbound calls should take.

Branded caller ID and anti-spoofing solutions

Branded caller ID and anti-spoofing solutions also increase call answer rates. Branding displays the caller's identity to consumers on outbound calls, while anti-spoofing reduces the ability of attackers to misuse a company's numbers or brand identity as a means of impersonating the business. Both measures help to increase a company's ability to reach consumers while also building trust.

These solutions are not perfect and must be combined with healthy calling practices to improve call deliverability. Nonetheless, they are an important step toward reducing the likelihood that consumers will perceive incoming calls from legitimate businesses as fraud.



Recommendations

Adopt consumer-friendly calling practices

Healthy calling techniques, such as avoiding repetitive calls to consumers who are not interested in answering them, reduce the risk that a call will be reported by users as spam or blocked. They also build customer trust and enhance the image of a business's brand in the eyes of consumers.

For specific guidance on consumer-friendly calling techniques, refer to Hiya's [Best Practices Calling Guide](#).

Inbound call protections

To reduce the risk of having their own employees fall victim to spam, fraud and deepfake calls, businesses can deploy inbound call protection technology. These solutions operate at the mobile device and network level, automatically monitoring for incoming threats.

The steps that some businesses have taken to help secure voice communications are encouraging—but, many are not yet acting as proactively as they could in the face of growing voice-based risks.

A Smarter, Layered Approach to Voice Security

No single solution can fully protect your business from voice-based threats. That's why a layered strategy is essential—combining identity

verification, scam call blocking, and spoofing prevention to reduce risk from all angles. Embedding these protections into your communication systems helps keep employees, customers, and partners secure—without slowing anyone down.

Understanding customer-friendly calls and reputation

Maintaining the integrity of business calls is essential in today's communication landscape. With the global rise in phone scams and fraud, consumers have become increasingly wary of unidentified calls. Retail and device manufacturers have responded up their efforts against invasive phone calls by implementing consumer protections such as

In this landscape, it's increasingly important to ensure their calls are customer-friendly. Both consumer preferences and applicable laws require companies to respect consumer rights. Customers want to hear from you; despite voice fraud and scams, phone calls remain a primary communication method for most businesses. By following customer-friendly calling practices, you can establish yourself as a trusted caller, improve customer satisfaction, and avoid common reputation pitfalls along the way.

This guide covers best practices for making phone calls, and why it matters for your company's reputation.

i

What is a customer-friendly call?

Calls are considered customer-friendly if they respect consumer preferences and rights.

What are call warning labels?

When it comes to call reputation, many consumers are understandably concerned about call warning labels.

Call labels serve as a first line of defense, helping them to identify suspicious calls. There are several primary types of call labels that users may encounter:

2 10 TIPS FOR A POSITIVE CALL REPUTATION

- Suspected scam / Likely fraud / Potential fraud:** Calls flagged as potential scams based on verifiable data and patterns recognized by carriers.

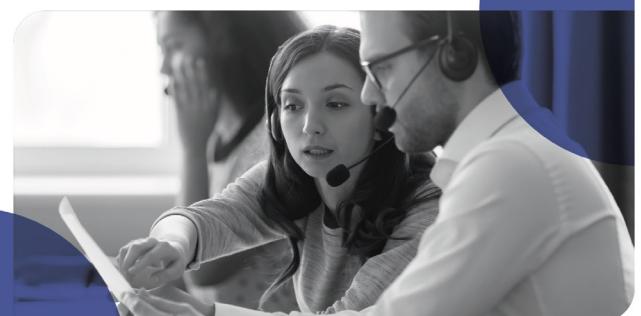
hiya

hiya

10 TIPS FOR A POSITIVE CALL REPUTATION

Ten tips to prevent reputation issues through customer-friendly calling practices

A HIYA BUSINESS BEST PRACTICES GUIDE



CONCLUSION

Making the world safe for voice calling

The data is clear: The world can't live without voice calling, which plays an absolutely vital role in facilitating high-stakes communications. Yet, too often, voice calls present challenges for both consumers and businesses, due to traditional risks like number spoofing as well as more novel and sophisticated types of attacks, such as deepfakes.

Solutions to all of these challenges are readily available—and many consumers and organizations are already taking advantage of them. But others are missing out and not taking full advantage of the call productivity and security protections available to them and their customers.

To safeguard the future of voice, now is the time to take action by deploying solutions that preserve voice as a safe, reliable, trustworthy means of communication.

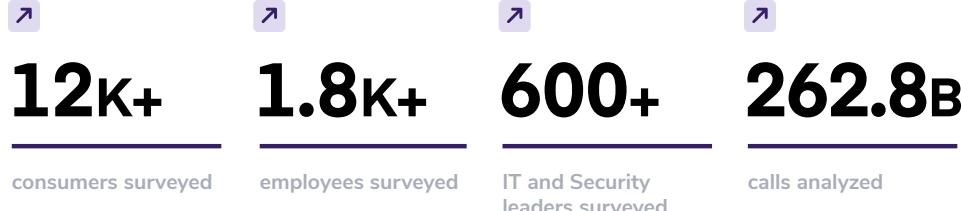
Methodology

Market research

Censuswide conducted market research on behalf of Hiya between December 24, 2024, and January 7, 2025. The survey included responses from 12,003 consumers, 1,802 workers who use a phone as part of their job, and 600 senior professionals with titles such as VP of IT or CISO. Respondents were based in the UK, US, Canada, France, Germany, and Spain. Censuswide is a member of the Market Research Society and adheres to its code of conduct, which is based on ESOMAR principles.

Hiya Data

Hiya's proprietary data for this report focused on the following countries: US, Canada, UK, Germany, France, and Spain. Hiya's data includes more than 262.8 billion calls that passed over its network in 2024. The Hiya Voice Intelligence Network includes more than 300 million users worldwide through Hiya's integrations with wireless carriers and device manufacturers, and the Hiya app. All proprietary data has been aggregated and anonymized.





Learn more at hiya.com

Hiya is trusted by global businesses, carriers, and consumers to provide secure, engaging connections and stop unwanted calls. Built on the world's leading Voice Security Platform, Hiya connects businesses with their customers, helps carriers secure their networks, and protects people from spam and fraud calls. Hiya's SaaS applications, Hiya Connect and Hiya Protect, serve more than 400 million users on the Hiya Voice Security Network, powering call protection and identity for AT&T, EE, Samsung, Ericsson and more.