Google

MARCH 2025

What comes next in the fight against unwanted phone calls?

What comes next in the fight against unwanted calls?

CONTENTS

ABSTRACT

This report dives into the persistent problem of unwanted calls and how the latest advancements in artificial intelligence (AI) can be used to detect suspicious behavior during a phone call.

The report explains the evolution of the unwanted telemarketing calls and fraudulent scam calls, explores the conversational tactics scammers use, and how various efforts across government, telecommunications providers, smartphone manufacturers, and third party developers are combating these unwanted calls.

Finally, the report examines how real-time detection and a warning system can protect users from falling victim to a phone call scams. Pixel is launching on-device AI to detect and warn users of suspicious behavior exhibited by potential scammers during a phone call before users divulge personal information or payment details.

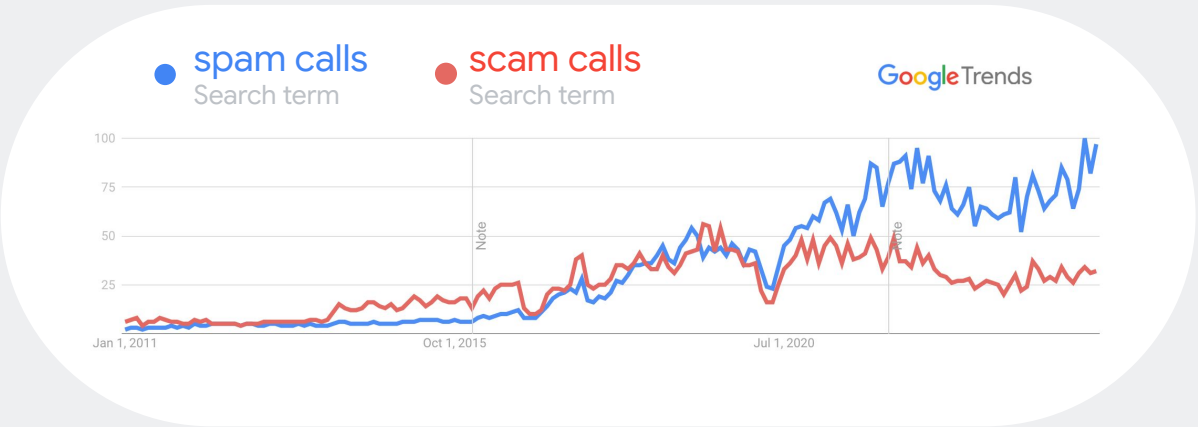
Scamming remains financially lucrative for bad actors. While it may never be fully mitigated, it can be managed. Google remains committed to developing and implementing solutions that leverage the latest developments in AI and other technologies to protect users around the world.

Introduction

Despite concerted efforts over decades, fraudulent calls offering extended car warranties, threatening legal action because of unpaid taxes, or asking for Americans' social security numbers still persist.

Google Trends has shown an increase in searches for 'spam calls' and 'scam calls' over the last decade. Americans frequently search for how to identify, stop, and block these unwanted phone calls.

> **Americans have been trying to protect their phone numbers from unsolicited telemarketers, spammers, and scammers for decades.**



The United States government, US telecommunications carriers, smartphone manufacturers, and downloadable third party applications have all tried to stop unwanted calls. In survey conducted by Qualtrics on behalf of Google, 40% of Americans still reported receiving multiple scam calls per day in 2024.

Why do unwanted calls still exist? How can Americans protect themselves from unwanted calls once and for all?

Understanding how scam phone calls are made

History of Unwanted Calls

It all got started when the world became connected

Phone calls were invented in 1876 to keep friends and family connected. In the late 1800s, phone calls became sticky because neither the "postal system nor the telegraph could provide everyday information as people created it and deliver it immediately to someone else."

As telephone wires were laid across the United States, more phones meant more and more people could be reached. The combination of network effect, long-distance reach, and immediacy was a catalyst for innovation. Different types of phone calls emerged throughout the decades.

Phone calls have been used for many purposes - to trade gossip, to announce the start of war, to book a flight on a commercial airline, or to call 9-1-1 for emergency assistance.

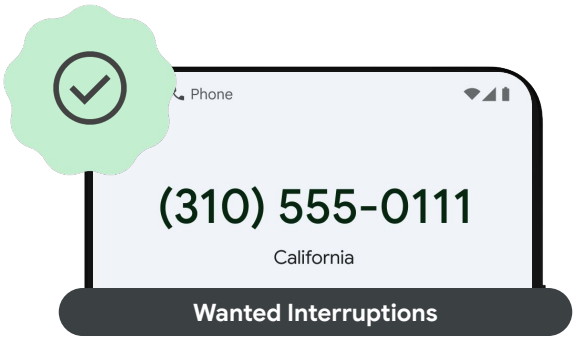
> **The benefit and drawback of the telephone was that a personal phone number offered direct *and immediate* access to users.**

This type of direct and immediate access would eventually be exploited by nuisance spammers and nefarious actors.

Unknown Callers

Disruptive, demanding interruptions

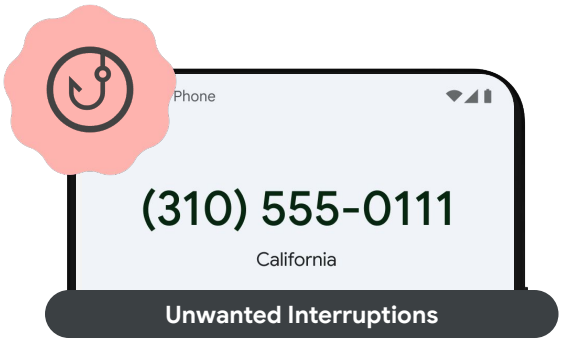
Incoming phone calls are disruptive because they require immediate attention. Within seconds, users must decide to answer, ignore, or decline an incoming call. These interruptions fall into two categories: wanted and unwanted interruptions.



Wanted Interruptions

Calls users want to answer because users have shared their phone number with the business or person.

Ex: Doctor's office, child's school, potential client, job recruiter



Unwanted Interruptions

Calls users do not want to answer because they did not share their phone number or no longer want to be contacted.

Ex: Unsolicited sales offers, fraudulent scams, and harassment

> **The challenge is deciphering if an incoming call from an unknown number is a wanted versus unwanted interruption.**

Without a universal set of yellow pages or caller ID, Americans rely on contextual clues such as area code and time of day to guess who might be calling from an unknown number.

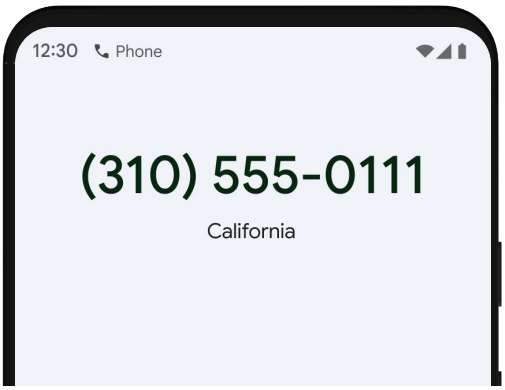
Time of Day

Received a call during a specific hour

Ex: Doordash delivery, Uber driver, job interview

Received a call during a expected window of time

Ex: Mechanic saying car is ready for pickup, vet sharing test results



Area Code / Location

Received a call from an area code where they do not know anyone

Ex: Foreign country, different state

Received a call from an area code that reflects where they used to live, not their current location

Ex: Different part of the state, different state entirely

Unknown Callers Impact

Unanswered calls

In a survey conducted by Qualtrics on behalf of Google, 40% of Americans receive multiple incoming calls from an unknown number daily. 69% of Americans find these calls to be bothersome interruptions.

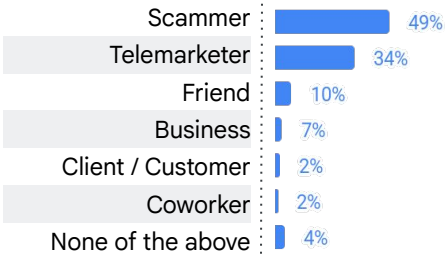
Based on their previous experience answering incoming calls, 83% of Americans expect an incoming call from an unknown number to be an unwanted call from either from a scammer or a telemarketer.

Therefore, it is not surprising that 60% of Americans say they typically reject or ignore incoming calls from unknown numbers. These Americans are tired of the constant influx of unwanted calls.

Yet, by ignoring calls from unknown numbers, they may unintentionally miss a call from their insurance provider or their doctor's office scheduling a follow up appointment.

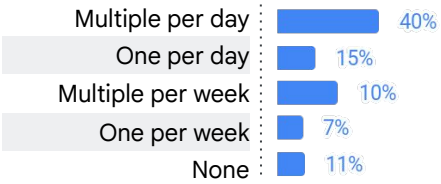
> **Users have developed a sense of learned helplessness due to the volume and frequency of unwanted interruptions.**

When you see an incoming call from an unknown number, who do you typically expect is calling?



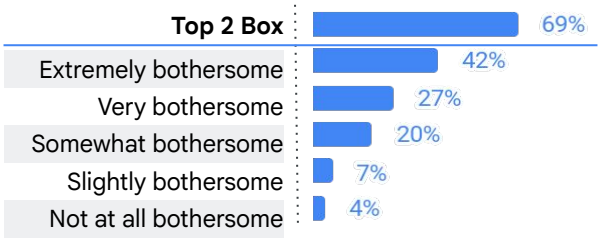
Source: Online Survey conducted by Qualtrics on behalf of Google, N=1,961 respondents, US, 18 years or older, Q4 2024

In the past week, how many phone calls have you received from an unknown number?



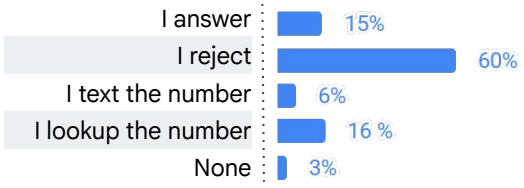
Source: Online Survey conducted by Qualtrics on behalf of Google, N=1,961 respondents, US, 18 years or older, Q4 2024

How bothersome do you find phone calls from unknown numbers?



Source: Online Survey conducted by Qualtrics on behalf of Google, N=1,961 respondents, US, 18 years or older, Q4 2024

When you receive a call from an unknown number, what do you typically do?



Source: Online Survey conducted by Google, N=662 respondents, US, 18 years or older, Q3 2023

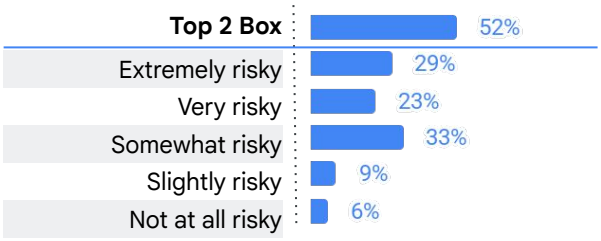
Ultimately, answering an incoming call from an unknown number increases the risk of speaking with a fraudster and falling prey to a scam operation.

More than half of Americans believe it is risky to answer an incoming call from an unknown number.

In fact, 42% of Americans answered an incoming call from a scammer in 2023.

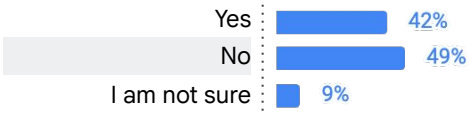
Finding a balanced approach to answering important phone calls from unknown numbers and minimizing contact with scammers is a common challenge.

How risky is it to answer an incoming call from an unknown number?



Source: Online Survey conducted by Google, N=551 respondents, US, 18 years or older, Q3 2023

In the past 12 months, have you answered an incoming call and spoken to a scammer?



Source: Online Survey conducted by Google, N=551 respondents, US, 18 years or older, Q3 2023

Spam Calls

Cheap phone calls at scale

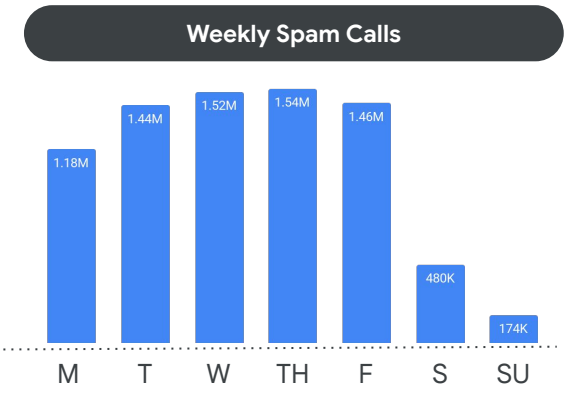
Unwanted phone calls emerged in the US in the 1980s. The first type of unwanted call was 'dinner hour marketing' otherwise known as telemarketing. Telemarketers strategically called families around dinner time because families were at home and near their landlines, typically located in the kitchen. Most landlines did not have caller ID, so when the phone rang, Americans had to pick up the phone and ask who was calling.

> **Fear-of-missing-out (FOMO) influenced user behavior because their insatiable curiosity wanted to know *who* was calling.**

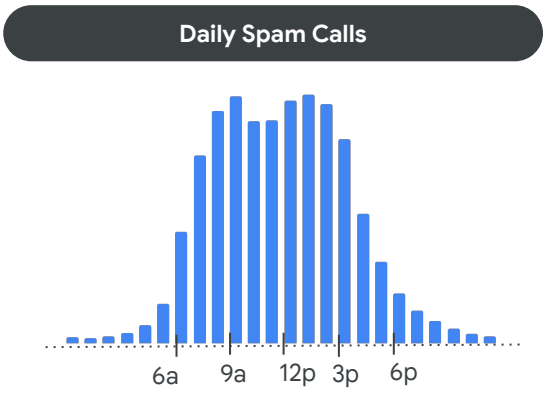
Those dinner hour marketing calls evolved into robocalls. Technology advancements allowed telemarketers to make mass calls with pre-recorded messages using autodialers. Recording one message and sending it out to millions of Americans was significantly more efficient than calling one million Americans individually. Robocalls were not only effective, they were lucrative. In 1991, Congress determined that telemarketers called more than 18 million Americans everyday and generated $435 billion dollars in 1990. In 1997, the Direct Marketing Association estimated that 34% of US sales had come from telemarketing. By 2003, telemarketers were calling as many as 104 million Americans everyday and generating an estimated $600 billion dollars.

> **The ability to reach users directly *at scale* for a relatively *low cost* created a ripe opportunity for spammers and scammers.**

Based on product analytics from Pixel's native phone application, spam calls are more frequent during business hours on weekdays. Spammers call on weekdays during business hours to disguise themselves as a potential business. Thursday is the most spammy day, while Sunday is the least spammy day of the week. Spam calls increase throughout the morning and peak at 1pm. Then the number of spam calls declines until midnight.



Source: Pixel Phone Application Analytics, Retrieved 2/24/25



Source: Pixel Phone Application Analytics, Retrieved 2/24/25

Spam Calls Impact

Bothersome and subjective

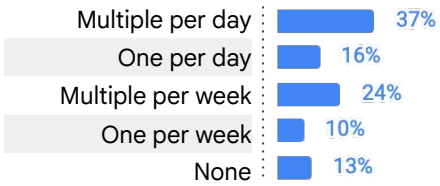
Two decades later, spam calls continue to bother Americans. 37% of Americans receive multiple spam calls a day. 47% of Americans find these calls to be extremely bothersome.

Most Americans expect an incoming call labeled as spam to be an unwanted call. But, spam is subjective. Users will report a phone number as spam if the caller was perceived to be a nuisance. Unfortunately, this behavior results in legitimate businesses being labeled as spam.

Consequently, 31% of Americans have missed at least one important call because it was labeled as spam.

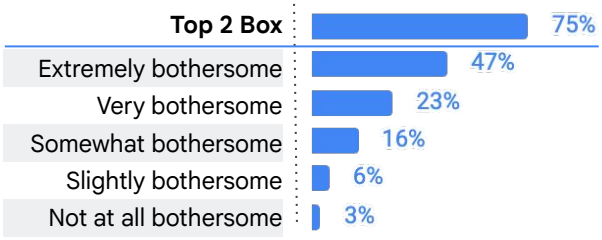
Overtime, the efficacy of labeling dwindles because spammers and scammers are constantly changing numbers.

In the past week, how many spam phone calls did you receive?



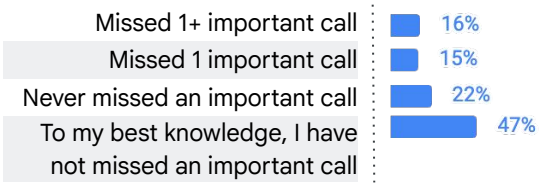
Source: Online Survey conducted by Qualtrics on behalf of Google, N=1,961 respondents, US, 18 years or older, Q4 2024

How bothersome are spam phone calls?



Source: Online Survey conducted by Qualtrics on behalf of Google, N=1,961 respondents, US, 18 years or older, Q4 2024

In the last 3 months, have you missed an important call because the call was incorrectly marked as spam?



Source: Online Survey conducted by Google, N=551 respondents, US, 18 years or older, Q3 2023

Scam Calls

Prevalent and growing problem

In the 2010s, the evolution of the spam robocalls into nefarious scam calls accelerated.

Scammers recognized that users were starting to avoid incoming calls from 1-800 numbers, incoming calls with unfamiliar area codes, or incoming calls that came up as 'unknown' on caller IDs. So, scammers started to spoof local numbers to entice users to answer incoming calls they might otherwise ignore.

Technology advancements in Voice over Internet Protocol (VoIP) made it possible for scammers to spoof calls with little technical knowledge at a low cost. Instead of pitching unsolicited offers, scammers began to prey on Americans' anxieties and scam users into sending money or sharing their personally identifiable information.

Scam Calls Impact

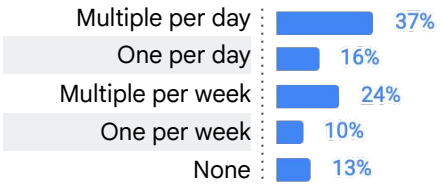
Financial and psychological harm

53% of Americans report receiving at least one scam call per day. Falling victim to a scam phone call results in both financial and psychology harm. As of Q3 2024, the Federal Trade Commission had received over 200,000 complaints about scam phone calls in the first three quarters of the year with Americans reporting $695M in losses from scam phone calls.

In user interviews with American scam victims, users reported a wide range of financial losses, from hundreds of dollars to several thousands of dollars, a significant depletion of their personal savings.

Not only did victims experience financial stress, they experienced an erosion of trust. Some reported feeling profoundly embarrassed that they were deceived and vulnerable realizing how anyone could fall victim to a phone call scam.

In the past week, how many scam phone calls did you receive?



Source: Online Survey conducted by Qualtrics on behalf of Google, N=1,961 respondents, US, 18 years or older, Q4 2024

Unwanted calls have become more than a nuisance, posing a real *financial* and *emotional* threat

Deconstructing the conversational scam call

Scam Operation

Low barrier to entry

Accessibility to personal phone numbers, low-tech setup, and readily available spoofing technology create an extremely low barrier to entry for scammers.

Personal Phone Numbers

How scammers get personal phone numbers

Personal phone numbers become potentially vulnerable during data breaches and are subject to being shared, leaked, and sold by unscrupulous brokers. Scammers obtain personal phone numbers through data brokers, data breaches, or from public profiles.

Spoofing Technology

How scammers go untraced

Scammers need spoofing technology to conceal their identities and proxy servers to disguise their internet protocol (IP) addresses making them less traceable to law enforcement. Scammers understand the limits of the law. They know they are even less likely to get caught if they target victims in a different country because there are limited international laws and enforcement agencies to dismantle and prosecute scammers across borders.

Scam Script

How scammers impersonate reputable businesses

Scammers create conversation scripts that leverage a hook, line, and sinker approach to impersonate reputable businesses, government agencies, or organizations to trick users that they have a plausible reason for payment.

Scammers target three different audiences and tailor scam scripts to those audiences to increase their chances of success.

Mass Market

Scam is broadly applicable to large general population

Ex: Scammers target mass audience with Amazon or Walmart scams

Semi-Target

Scam is tailored to a specific niche audience's vulnerabilities

Ex: Scammers target older Americans with Medicare and Social Security scams

Individuals

Scam is tailored to a specific individual

Ex: Scammers target a grandparent and may use artificial intelligence (AI) voice cloning to impersonate a loved one in distress

Scammers target users' vulnerabilities to induce feelings of fear, confusion, or opportunity and increase users' likelihood for falling victim to the scam. It is difficult for users to keep up with the latest scams because scammers are constantly seeking new vulnerabilities to prey on and are evolving their scripts.

The following are examples of vulnerabilities that scammers will exploit:

Government

Vulnerability:
Unpaid taxes

Scammers impersonate the IRS and demand victims pay overdue money to avoid arrest or deportation

Bank

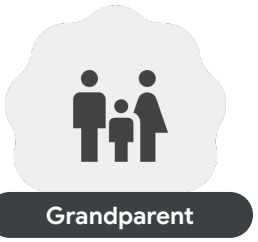
Vulnerability:
Unauthorized purchase

Scammers impersonate bank representative who is calling to flag a suspicious transaction to obtain login credentials to wire money

Tech Support

Vulnerability:
Dangerous malware

Scammers impersonate reputable tech companies, such as Microsoft, and claim the users' computer has been infected with malware



Grandparent

Vulnerability:
Distressed grandchild

Scammers impersonate a grandchild calling their grandparent requesting money to pay bail, insurance, and/or legal fees because of an accident

Retailer

Vulnerability:
Unauthorized purchase

Scammers impersonate Amazon claiming there are fraudulent charges on their Amazon account and request their credit card to verify their account

Employment

Vulnerability:
Unemployment or increased salary

Scammers impersonate recruiters and request payments for training materials or work-from-home supplies

Donations

Vulnerability:
Benevolence

Scammers impersonate community organizations such as a firefighters' union and claim they collecting donations to increase local funding

Sweepstakes

Vulnerability:
Lucrative winnings

Scammers impersonate a sweepstakes company and request users to pay fees to claim their winnings

Top scams differ across countries because scammers tailor their scams to exploit the top vulnerabilities of the market. For example, during the US presidential election in November 2024, scammers targeted Americans with election scams. In the UK, the price of gas and electricity surged post-pandemic. Thus, scammers targeted UK users with energy related scams. South Africa has one of the highest unemployment rates in the world at 31%, so thus scammers have targeted South African users with job employment scams.

Local Language

How scammers scale across borders

Scammers will target users who speak the scammer's native language or a second language the scammer has learned in school, such as English. This is why we see a high propensity of scams in English speaking countries such the US, Canada, Australia, and the United Kingdom.

Payment

How scammers get paid

Scammers target over 42 countries around the world. Scammers target countries with high gross national income (GNI) because those countries have strong currency, affluent users, and widespread adoption of digital payments methods. However, scammers will also target countries with low GNI because low income users can be more susceptible to money making scams in hopes of improving their financial situation.

Scammers seek financial gain through irreversible and real-time payments such as wire transfers, gift cards, cryptocurrency, or cash deposits into a fraudulent ATM account. The widespread adoption of digital payment and mobile banking apps has allowed conversational phone scams to explode in the last decade compared to the early 2000s when it was not as straightforward to send real-time payments.

Impact

Low barrier to entry with high payoff

Scammers are effective. According to the Global Anti-Scam Alliance, scammers stole over $1.03 trillion from victims in 2024 through email, text messages, social media, and phone calls scams. Scam phone calls will continue to persist so long as the time, effort, and risk are worth the financial gain.

> **Low barrier to entry**
> **+ high financial reward**
> **+ low probability of getting caught**
> **= a situation ripe for scams.**

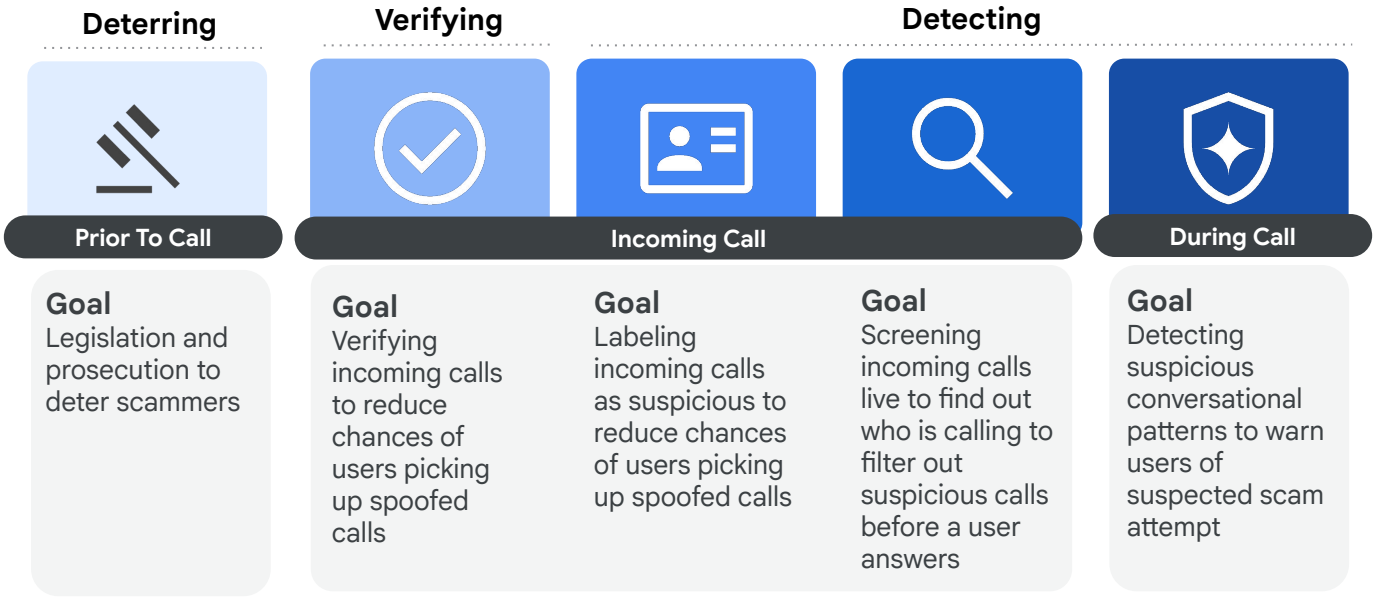
Finding ways to combat scam calls

Current Solutions

Understanding the solution landscape

To effectively combat phone scams, it is crucial to disrupt the economic incentives that drive them. Fundamentally, the costs associated with perpetrating a scam must consistently outweigh the potential benefits. This can be achieved through a multi-pronged approach:

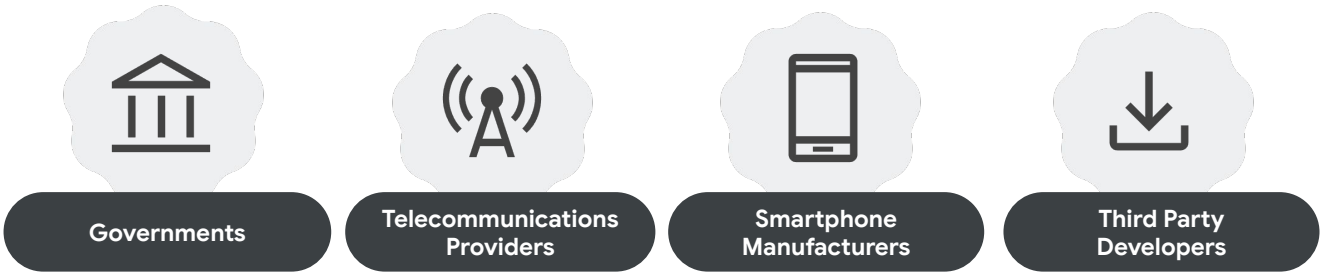
- **Deterring scammers through increased risk**: Enhancing law enforcement efforts to substantially increase the probability of scammers being identified, caught, and held accountable. Increased risk elevates the perceived cost of engaging in scamming activity.
- **Increasing scammer operational costs**: Imposing higher costs on the infrastructure and resources needed to initiate and execute scams, such as, access to spoofing technology, call center operations, or other essential elements of the scamming process.
- **Reducing scam success**: Implementing strategies to reduce the probability of a user falling victim to a scam. Strategies include solutions that empower users to recognize and avoid scams.



Multiple Entities

How different entities are combating unwanted calls

Multiple entities have recognized the magnitude and frequency of scam calls and have actively been trying to combat unwanted calls. Some examples include governments, carriers, smartphone manufacturers, and third party developers.



Governments	Telecommunications Providers	Smartphone Manufacturers	Third Party Developers
✓ **Designing industry-wide technological solutions** to reduce spoofed calls	✓ **Offering protection features** that enable users to manage incoming calls	✓ **Offering protection features** that enable users to manage incoming calls	✓ **Offering protection features** that enable users to manage incoming calls
✓ **Enforcement actions and penalties** that outweigh the monetary gains	✓ **Labeling incoming calls** as suspicious to deter answering suspicious calls	✓ **Labeling incoming calls** as suspicious to deter answering suspicious calls	✓ **Labeling incoming calls** as suspicious to deter answering suspicious calls
✓ **Generating awareness** of scams and user education on how to stay safe	✓ **Implementing solutions** that make it harder for scammers to operate	✓ **Generating awareness** of scams and user education on how to stay safe	✓ **Generating awareness** of scams and user education on how to stay safe
✓ **Collaboration with industry** to track down and prosecute scammers	✓ **Cooperating with government** efforts to track down and prosecute scammers	✓ **Ensuring that devices** can effectively utilize anti-scam technologies	

Deterring Scammers

Legislation and prosecution

Legislation and prosecution play an important role in combating scam calls.

The US government, regulatory agencies, and states have taken several steps to combat unwanted calls, increase the likelihood of scammers getting caught, and disincentivize scammers by imposing penalties that outweigh the monetary gains. Here are some example of steps they have taken in this direction:

Establishing regulatory frameworks

The Telephone Consumer Protection Act (TPCA) enacted by Congress restricts telemarketing calls with the use of automatic telephone dialing systems and prerecorded voice messages to protect users from unsolicited robocalls.

The Federal Communication Commission (FCC) and Federal Trade Commision (FTC) have required gateway providers to stop illegal robocalls that originate overseas.

Increasing ability to find scammers

The TRACED Act was created to provide the FCC with greater authority to deter criminal robocalls.

FCC has collaborated with industry groups to trace back scam calls to their origins to identify the perpetrator.

Enforcing fines and penalties

The Federal Trade Commission (FTC), Federal Communication Commission (FCC) Department of Justice, and attorneys general from every state have made efforts to stop robocalls. Scammers and companies that facilitate scammers have been hit with restraining orders, fined, sued, arrested, and sent to prison.

The FCC has imposed fines for illegal robocalls using deep fake AI generated voices.

As of February 2025, the FTC has resolved 147 of 151 enforcement actions against violators of the Do Not Call, robocall, spoofed caller ID, and assisting and facilitating violations. They recovered over $178 million in civil penalties and $112 million in restitution or disgorgement.

Legislation and prosecution is an important aspect of protecting users from unwanted communication.

Verifying Incoming Calls

Authenticating to reduce spoofing

Scammers use Caller ID spoofing to mask their identity and make it appear that the incoming call is from a legitimate company, government agency, or even someone's family member. To solve this problem, US regulators introduced STIR/SHAKEN, a series of protocols and procedures to crack down on Caller ID spoofing by verifying the origin of the phone call. Under STIR/SHAKEN, mobile carriers are required to assign an attestation for every incoming call. The highest level of attestation acts as a stamp of legitimacy authenticating the call.

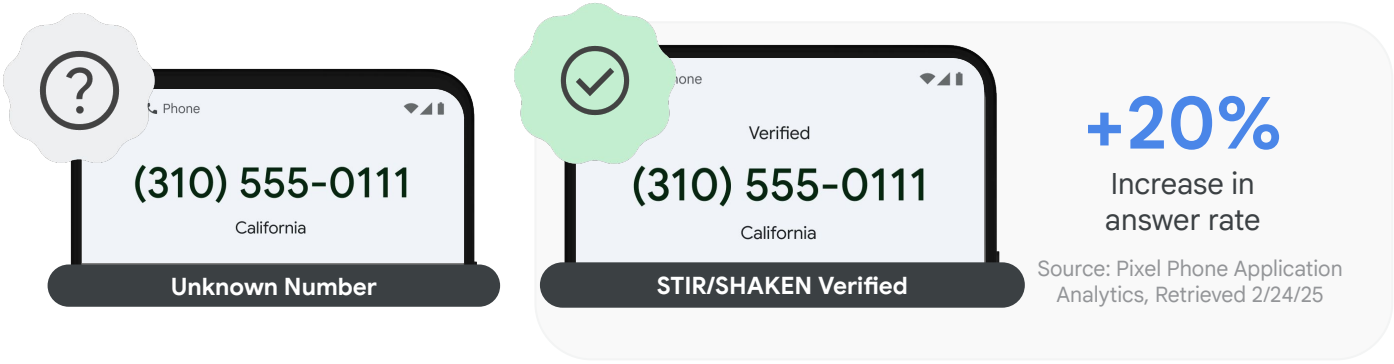
Impact

Increased answer rate

Phone by Google uses STIR/SHAKEN in the following two ways:

1. Users of the Phone by Google application may see a checkmark or verified label if the call is verified by this protocol
2. The signal that the call is verified is also used in spam and scam detection models to improve accuracy of a prediction that the call is a likely spam or scam

STIR/SHAKEN verification builds users' confidence that an incoming call from an unknown number is trustworthy and leads to an increased answer rate for legitimate calls that were verified with this protocol.



Unfortunately, not every incoming call in the US has an attestation level. STIR/SHAKEN authentication does not authenticate calls from older non-IP networks and is not able to authenticate international calls well (as it is implemented only in the US and Canada). Additionally, this protocol verifies the origin of the call (the originating provider) and the integrity of the call information during transit. It does not inherently verify the legitimacy of the caller ID itself. This means a scammer could still spoof a number, and the call could be signed as legitimate if it originates from a network provider who signed this call with a high attestation level.

> **STIR/SHAKEN increases trustworthiness and call answer rate, but is not available for all calls.**

Labeling Suspicious Calls

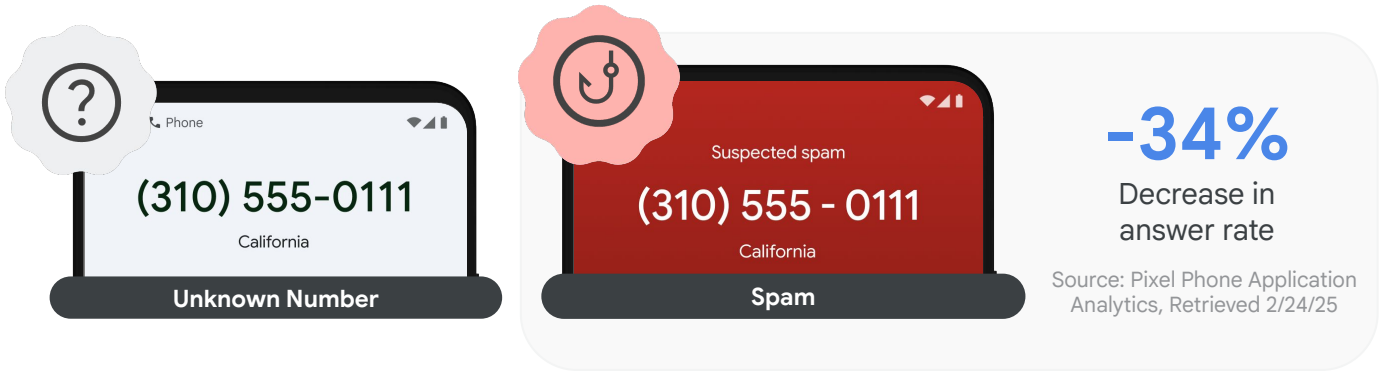
Labeling incoming call as suspicious

Carriers, smartphones manufacturers, and third party downloadable applications leverage user reporting to understand if a phone number was suspicious or a nuisance. This user reporting is used to inform other users if the incoming call is likely suspicious.

Impact

Decreased answer rate

To reduce the opportunity for a user to get scammed, Phone by Google shows a warning on the incoming call screen to deter users from answering possible scam calls. This type of identification helps users infer if an incoming call is a wanted or unwanted interruption.



However, this approach has limitations because user reporting is subjective and because scammers spoof and rotate phone numbers quickly.

Firstly, what is perceived to be a nuisance caller to some, such as car dealership following up with a potential buyer, may be a legitimate and desirable caller to others. Secondly, scammers often spoof or rotate phone numbers and those numbers do not get enough spam reports in time to signal a warning to users.

> **Labeling an incoming call as a potential spam or scam increases the likelihood that a user will ignore the incoming call, but it does not stop all unwanted calls from reaching users.**

Screening Suspicious Calls

AI filtering to weed out unwanted calls

To stay safe from scammers, users will avoid answering calls from unknown numbers. At the same time, solutions like silencing all unknown numbers result in users missing important calls from unknown numbers, like doctors' offices, rideshare drivers, or delivery services.

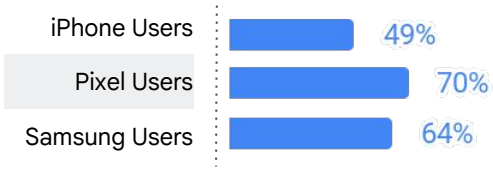
To avoid missing urgent calls and to receive real-time information about who is calling and why, Pixel launched Call Screen. Call Screen uses a friendly AI bot to answer an incoming call and displays a live transcription of the conversation so that the user can decide to answer or ignore. By default Call Screen can be triggered manually: users decide which incoming calls to screen. For advanced protection, Pixel users can enable automatic Call Screen in their Phone by Google application settings. It has three levels of protection and the highest level of protection will automatically screen all incoming calls from unknown numbers.

Impact

Increased user satisfied and protection

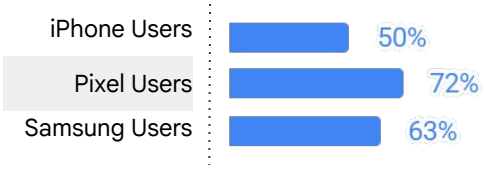
Led by Call Screen, Pixel's suite of protective features is effective. A survey conducted in Q4 2024 by Qualtrics on behalf of Google uncovered that Pixel users reported the highest level of satisfaction with their scam call protection and their feeling of protection compared to other smartphone users.

Overall, how satisfied are you with your protection from scam phone calls?



Source: Online Survey conducted by Qualtrics funded by Google, N=609 Pixel Users, N=3086 iPhone users, N=2426 Samsung Users, US, UK, JP, 18 years or older, Q4 2024

Overall, how protected do you feel from scam phone calls?



Source: Online Survey conducted by Qualtrics funded by Google, N=609 Pixel Users, N=3086 iPhone users, N=2426 Samsung Users, US, UK, JP, 18 years or older, Q4 2024

Screening incoming calls identifies who the *caller claims to be*, but cannot verify their identity. Scammers impersonate reputable businesses making it difficulty to screen for authenticity.

Alerting During Suspicious Calls

Conversational AI intelligence to detect scam attempt

A survey conducted by Finra Foundation in September 2019 with Americans and Canadians demonstrated that third party interventions during the scam help victims avoid losing money. In fact, 51% of victims who experienced an intervention were able to avoid losing money. Interventions in the study included bank tellers, cashiers, or employees trained to recognize fraud such as large cash withdrawals or high-dollar gift cards.

> **Intervention is the last moment to protect users from falling victim to a phone calling scam.**

If a user decides to answer an incoming call from an unknown number, there will always be a risk the user could fall victim to scam. Users need a solution to intervene and alert of suspicious behavior during a phone call.

Pixel's Scam Detection uses on-device, real-time detection to identify suspicious conversational requests and social engineering tactics commonly used by scammers. If the model detects suspicious activity, the feature intervenes with a visual, sound, and haptic alert to warn the user.

Scam Detection is built to protect users' privacy and ensure they are always in control of their data. The solution is off by default to give users control over this feature and it is never on during calls with saved contacts. Call audio is processed ephemerally and no conversation audio or transcription is recorded, stored on the device, or sent anywhere else.

Impact

Timely intervention increases caution

Pixel's Scam Detection was released to Public Beta in November 2024. Based on an in-application survey conducted in Q4 2024, users found the scam alert useful because the alert increased caution and protected them from falling victim to a scam.

Pixel Public Beta users said the scam alert made them ***more*** cautious

Source: Pixel Phone Application, in-app survey conducted by Google, N=400 respondents, US, 18 years or older, Q4 2024. Other 51% found the alert useful for different reasons.

> **A real-time scam alert can protect a user from a scam attempt before divulging personal information or initiating payment.**

The Future of Phone Call Scams

More prolific in the years to come

Scam phone calls are an unfortunate reality for our digitally connected world. It is a scattered and far-reaching problem that is difficult to track and pin down, even as governments and authorities try to prosecute rings of scammers. How can Americans stop receiving scam phone calls once and for all?

> **Scam is like crime. Unwanted calls can be managed, but might never be obsolete.**

History has already begun to repeat itself. Just as robocalls became prolific because advances in technology allowed telemarketing to become progressively cheaper and easier to scale, the same is happening with scams. Based on our research and work with financial institutions around the world, phone calling scams will likely become even more prolific in the coming years because advances in AI will allow scammers to scale their operations for a relatively low cost.

- Scammers will likely use AI voice-cloning to create deep-fake voices to conceal their identity, appear more authentic, or impersonate an authoritative figure.
- Scammers will likely use large-language models to write new conversational scam scripts to avoid triggering the detection algorithms that rely on known conversational patterns.
- Scammers will likely use large-language models to translate their conversational scripts into multiple languages to reach a wider audience.
- Lastly, scammers will likely continue to leverage spoofing software and auto dialers to call thousands of users at scale, skirting international law, and making it difficult to trace the origins of the call.

Combating a problem of this magnitude requires shared accountability across borders, governments, law enforcement agencies, telecommunication carriers, and smartphone manufacturers. There is opportunity to share scam knowledge and emerging trends across entities to refine scam detection algorithms and accelerate public awareness campaigns.

> **Google remains committed to developing and implementing solutions that leverage the latest developments in AI and other technologies to protect users around the world.**

© 2025 Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043.