The Definitive Guide to Reducing Robocalls

Follow these steps to cut back on calls everybody loves to hate

You've had it with relentless robocalls, the automated messages that at best are telemarketing and at worst are pitches from criminals who want to steal your cash or your identity.

Enough is enough with the deluge of unsolicited voice mails and the calls from phone numbers that look like they're local but are spoofed (or disguised) by crooks who claim to be with the IRS or to have important information about your car warranty.

You've tried blocking numbers, to no avail. You've signed up on the National Do Not Call Registry. No difference. You've complained to the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC). Nada.

Scam calls rebound from COVID crash

When the coronavirus pandemic erupted in early 2020, "we saw the first major drop in robocalls because call centers were closed, but now robocalls are exploding," says Alex Quilici, CEO of YouMail, which develops robocall-blocking software.

Robocall volume in the U.S. hit an estimated 5.7 billion calls — an all-time high — in October 2019, then sank to about 3 billion a month in the spring of 2020, according to YouMail's Robocall Index.

Spammers and scammers have since rebounded, with robocalls averaging 4.1 billion a month over the past year. That's more than 1,500 calls per second.

"Having computers dialing a bunch of numbers is a fast, efficient and extremely cheap way to get to as many people as possible," Quilici says, adding that scammers need only a tiny slice of call recipients to respond for their endeavors to pay off.

Some robocalls are legal

Amid the din, some robocalls are legitimate. Charities, pollsters and medical-service providers are among those who can legally autodial you. The American Red Cross can robocall you to ask for blood donations, for example, and your doctor's office may do so to remind you of an appointment.

But when it comes to bad actors, keep in mind that mobile apps can beat them back. Also, importantly, the FCC now requires voice-service providers to implement call-authentication technology on the Internet Protocol (IP) portions of their networks.

The James Bond–sounding “STIR/SHAKEN” authentication enables providers to verify that the caller ID information transmitted matches the caller’s real phone number. This anti-spoofing step was mandated by the federal TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act, an AARP-endorsed measure signed into law at the end of 2019.

On the corporate side, the trade group USTelecom established the Industry Traceback Group to identify the sources of illegal robocalls and work with governments to “bring to justice individuals and entities responsible,” says Patrick Halley, USTelecom’s senior vice president of policy and advocacy. The source of an illegal robocall — even one from outside the U.S. — often can be identified in 24 hours, Halley says. While billions of illegal and unwanted robocalls are still placed annually, fewer of them are reaching consumers, thanks to call-authentication, call-blocking and call-labeling tools that designate incoming calls as spam, he says.

For example, AT&T, the largest U.S. carrier, says it is blocking more than 1 billion robocalls a month.

Best practices for consumers

To join in the fight, consumers are urged to:

Download a call blocker. First, try a free solution to see if it does the trick. No-cost services from firms such as YouMail and Nomorobo are carrier-agnostic. (Nomorobo is free for landlines but $1.99 a month for cellphones.) Your mobile carrier has free tools, too.

Experiment with call-blocking tools, apps and options, to strike the right balance between the calls you want and those you don't. It may take trial and error to avoid a "false positive," the term for a legitimate call that is stopped.

Let a call go to voice mail if it gets through a robocall app and you don't recognize the caller. If the caller claims to be from, say, Citibank, don't call back a number left on voice mail. Use a number that you know is legitimate, such as one on a statement or credit card.

Hang up if it's a live person calling, as computer-based robocall systems allow. Do not engage.

AT&T

AT&T Call Protect blocks all known fraud calls outright, while suspected spam is labeled so users can choose whether to answer. The company says it blocks or labels about 1 billion robocalls a month.

For a fee, users can download an advanced version of the Call Protect app that includes caller ID and allows users to block, allow or send certain call types to voicemail.

The company's fraud team uses machine learning to identify suspicious call patterns and prevent illegal calls.

AT&T uses automated scanning to identify and help block spam.

T-Mobile

T-Mobile and Sprint cellular plans include Scam Shield, a free set of tools that alerts users when a call is likely a scam and blocks calls the network considers to be more serious threats.

Its plans now include free caller ID.

Customers receive a free "proxy telephone number," a second number to give out when looking to keep one's main number private.

Customers are allowed a free number change if their current one becomes a magnet for excessive spam calls.

Verizon

Most Verizon wireless customers have access to Call Filter, a free app that automatically blocks what the company determines are likely fraudulent calls.

Verizon offers Call Filter Plus for an additional fee. The app allows users to create a list of numbers to block. It also includes caller ID, access to a database of 100 million known spam callers, and a visual spam risk meter. Verizon has created fake “honeypot” lines to track illegal robocall campaigns and notify law enforcement, says spokeswoman Kate Jay. As of late 2021, the lines had revealed more than 250,000 scams, Jay says.

— Joe Eaton
by Marc Saltzman