The Washington Post

Die Robocalls Die: a guide to stop spammers & exact revenge

By Geoffrey Fowler, Published: April 7, 2019

We tested six apps and services to find the best way to fight back against bots, telemarketers and fraud.

Robocalls, those computer-generated shysters, are making some people stop answering the phone altogether. The rest of us trust unknown calls about as much as truck-stop sushi. By several estimates, Americans got more than 5.2 billion automated calls in March – a record of about 16 for every man, woman and child.

It's happening because the Internet made it incredibly cheap and easy to place thousands of calls in an instant. But we don't have to just bury our heads in the spam and take it. While lawmakers debate what to do about the robo-scourge, engineers have cooked up clever ways to make bots work for us, not against us. Verizon just started offering free spam-fighting technology like AT&T and T-Mobile, if you sign up. The right app or service on your phone can make it safer to say hello again – or even exact revenge.

Yes, revenge.

So let's battle, bots. I collected dozens of robocalls from my Washington Post colleagues along with the (good grief) 30 I received in March. I get lots in Chinese. One colleague gets one for a "medical-grade brace" he definitely doesn't need. Then I took this list of 100 naughty numbers – and a few legitimate calls such as pharmacies and schools – to six tech companies that flag and block robocalls on cellphones: Hiya, Nomorobo, RoboKiller, TNS, Truecaller and YouMail. (Landlines and VoIP phones also get barraged, but some of the solutions are different.)

My test lasers in on one important question: Who was first at identifying the bad guys? I discovered no service could flag more than two-thirds of the calls on my list, in part because so many robocalls spoof their identities. Those are the calls that look conspicuously similar to your number, or that copy the caller ID of some poor soul who gets lots of angry return calls.

In a robocall deathmatch, speed matters. And one free app was, on average, faster at adding bad guys to its blacklist.

It comes down to how much effort you want to put into battling robocalls and how much personal information you're willing to share to make it happen. Just adding numbers to your phone's individual block list won't get you very far, but there are a few simple steps from which everyone can benefit. Here's my recommended plan of attack.

Round 1: Register on the Do Not Call list.

It won't help much, but it takes 30 seconds, so why not? The list, kept by the Federal Trade Commission, tells legitimate telemarketers not to bother you – the equivalent of a "no trespassing" sign on your lawn. Bonus: It also registers with the government that you care about this issue. It's free to register at **donotcall.gov**.

Round 2: Activate your service provider's free protection.

Phone companies have finally realized that stopping robocalls is an essential part of what we pay them for.

You may have heard recently that the biggest carriers pledged to support new network technology with a James Bond name – STIR/SHAKEN – that will help identify the true origin of calls. That's a good thing to help stop all those spoofed calls, but there's still a lot to work out before it might make a noticeable difference.

Meanwhile, everyone should take advantage of technology the carriers offer to identify and block certain robocalls. AT&T, T-Mobile and Verizon offer free services that monitor network activity and crowdsourced reports to block suspected fraudulent calls. The carriers outsource these services to Hiya, First Orion and TNS, respectively.

Don't worry, they cross-check your contacts list to make sure they don't block someone legitimate. One caveat: If your company pays for your phone service, it might have to authorize turning on some of these services.

AT&T: Download an app called **AT&T Call Protect**. The free level of service will label suspected spammers and gives you the option to automatically block calls that are a fraud risk. Unfortunately, if you also want to automatically block nuisances like spam, political calls and telemarketers, you have to pay $4 per month, which comes with access to AT&T's mobile security service.

Verizon: Download an app called **Verizon Call Filter**, available now for iPhones and coming in a few weeks for Android. As of last week, Verizon stopped charging for basic service, which labels suspected robocalls and gives you three options based on risk level for how many to block. (Don't let Verizon's outdated description in Apple's app store confuse you; there really is a free version now once you download the app, and

there's no need to sign up for a 10-day free trial.) If you pay $3 per month, you'll also get caller ID.

T-Mobile: Most T-Mobile customers already have the company's **Scam ID** and **Scam Block** service turned on, with no need to download an additional app. If you pay $4 per month, you'll get better caller ID and the ability to send more kinds of calls straight to voice mail.

In my test, the carrier services were slower at adding spammers to blacklists than some independent apps – and paying for their premium versions won't make them faster. In everyday use, these services take advantage of algorithms that might have stopped spoof numbers my test didn't pick up.

Verizon's service provider, TNS, and AT&T's provider, Hiya, identified nearly the same number of robocalls, though Hiya was a bit faster on average. (T-Mobile's provider, First Orion, declined to participate.) Just as important: Both let legitimate calls through.

Round 3: Get a robocall-blocking app.

If your carrier isn't squashing enough spam, independent apps offer a few tricks of their own. However, they're not all effective, and they might be after the personal data on your phone.

Into my bot battle, I threw four popular apps: **Nomorobo**, **RoboKiller**, **Truecaller** and **YouMail**. I also spoke with the companies behind them about how they make money and handle our privacy.

I recommend starting with the free **YouMail**, which won my robocall speed test. The main reason it's faster is that it has data carrier-provided services don't – the contents of your voice mail. YouMail replaces your phone's existing voice-mail service, and uses software to identify when robocallers leave messages – like Shazam for spam. That helps it quickly crowdsource the identity of new robocallers and block them from other phones.

If YouMail, which has about 10 million registered users, sees a scam rotating through many spoofed numbers, it knows not to block the numbers that belong to legitimate callers for all its users. A coming update will also allow you to automatically block spoof calls designed to look like they're coming from neighbors.

My favorite part: YouMail tries to trick known robocallers into taking you off their lists by playing them the beep-beep-beep sound of a dead line.

I wouldn't blame you for being hesitant about handing over so much data, including (on Android phones) the details of every call that comes in. You're required to use the

YouMail app to listen to your messages, but it does helpfully transcribe them, make them accessible online and offer fun outgoing message options. YouMail says it makes money through selling a premium voice-mail service for businesses and through advertising, but over its 12-year history, it also has run an identity-verification data service. The company told me it's ending its data business and won't sell user data or share it with others unless it's part of an effort to stop robocalls.

If you don't want to give up your voice mail, the most effective option is **Truecaller**, which replaces your phone's main call app and crowdsources spam numbers from about 300 million users worldwide (including 10 million in the United States). However, it wasn't my favorite app because you have to pay $3 per month to automatically block top spammers, and it stuffs in a lot of functions unrelated to robocalling.

The simplest app, at $2 per month, is **Nomorobo**, one of the first robocall blockers on the market with a popular service for home lines. Nomorobo doesn't sell your data or monkey around with your voice mail or calling apps, and it's smart about blocking spoofed calls that appear to be from neighbors. That said, I found it was the slowest to add my test's robocalls to its blacklist.

Round 4: Get revenge.

For some, dark times call for dark measures. The $4 per month **RoboKiller**, which ranked second in my speed test, takes over and fingerprints your voice mails but adds a clever twist – "answer bots." They're voice-mail messages that try to keep robots and human telemarketers on the line listening to nonsense.

Answer-bot options range from President Trump impersonators and extended coughing sessions to someone doing vocal exercises. Even better, RoboKiller will send you an often-hilarious recording of the interaction. (It only uses these recordings when it's sure it's a spam call.)

Another service, **Jolly Roger**, doesn't sell itself as a robocall blocker but takes this auto-generated-annoyance idea a step further by actively trying to game the spammers' systems, such as when to press 1 to speak to a human. It calls this tech "artificial stupidity." It costs $11.88 per year.

It's possible you're better off not engaging with a robocall in hopes the dialer will decide the line is dead. It's also not clear how much these cost the people placing robocalls. Time robocallers spend with your bot might be minutes they're not calling someone else, so you can think of it as community service.

I expect we'll see more software that works like this. Google's Pixel phones last year added a button to have a robot assistant screen calls. Even if you're not interested in revenge, good bots can play a role in combating bad ones.

How do you stop robocalls to your landline?

By Geoffrey Fowler, Published: April 10, 2019

It's not much of a stretch to describe robocalls as 2019's No. 1 tech problem.

Landlines

"We get calls in the middle of the night," writes reader Shulamit Elson in New York City. They appear to come from Slovenia and Kazakhstan and ring once before hanging up. In a recent column, I wrote about technologies that can help flag and block robocalls – and even exact revenge on the groups that make them – on smartphones.

But what about landlines?

I hear you. I've gotten dozens of questions about this from Post readers through my Help Desk form, email and Twitter. (Keep the horror stories coming, subscribers – your questions inform my investigations and reviews, and I'll try to answer the common and big thorny issues.)

Robocalls are certainly a nuisance to home phones, too, but the tech to stop them isn't as advanced. Some providers, such as Verizon, label suspected spam calls on a phone's caller-ID screen or let you block individually annoying numbers, but most home phones don't have access to apps that can be the brains of the operation. Landlines also run on diverse technology: Most Americans who still have a home phone use VoIP (voice-over-Internet) service, but 11% of homes still get service from old copper wire tech, according to U.S. Telecom, an industry trade group.

For most people, I recommend starting with a service called **Nomorobo**. It also sells a $2 per month smartphone app, but its roots are in landlines, where it is free.

Nomorobo does not work with copper-based phone lines. But it does work with dozens of VoIP carriers, including AT&T U-verse, Verizon Fios, Comcast Xfinity and Cox. I haven't tested it myself, but I know happy customers and have interviewed the company about its data practices and business. The company won a robocaller-tech contest run by the Federal Trade Commission a few years ago.

It works using a system called "simultaneous ring," which makes incoming calls to you also go to Nomorobo. If Nomorobo picks up first, its system tries to determine if it's a robocaller. If it is, your phone won't ring after that first time – and you'll know it squashed some spam.

If it's a legitimate call, they'll patch it on through to you. You just have to remember to wait for the second ring.

How does Nomorobo determine if it should hang up? It keeps a constantly updated database of about a million numbers with its own "honey pot" of phone lines that get lots of robocalls and crowdsourced reports from its users. In my tests of its smartphone app, Nomorobo wasn't as fast at identifying the bad guys as some competitors. But it was pretty good about not blocking legitimate robocalls, like from a pharmacy or school.

One thing to know: The product is free and – as I've written before about technology – that means it wants something from you. Nomorobo takes the data it gathers from landlines and uses it to figure out who to block from its paying smartphone customers. Nomorobo says it doesn't sell that data and uses it only to combat robocallers, so it's a decent exchange.

What if you have a copper phone line? Those require physical hardware you attach to your phone that screens out a list of known bad numbers. The problem is, the numbers scammers use change frequently. I haven't tested these devices, but ones such as the $100 CPR Call Blocker V5000 only come preloaded with 5000 numbers – a drop in the bucket for the 2019 robocall epidemic.

Beware of devices or services that rely on you to manually block numbers as robocalls come in. The robocallers might be spoofing legitimate numbers you might not want blocked some day, like tech support or government agencies.

Post readers have been sharing a few other interesting solutions. "I formatted my home phone to ring only twice so when the computer or whomever, hears my message, quickly hangs up and leaves no message," writes Judith Nathan of Leominster, Mass.

James Fullerton of Leesburg, Va., writes he doesn't get robocalls on his business line because he uses an "interactive voice response" system, also known as phone tree. "Robocallers simply can't decipher the greeting, hear the list of options/extensions, and therefore the IVR blocks 100 percent of robocalls with no further intervention required," he says. "The drawback is that the setup is somewhat complex."