ALERT: BEWARE OF THESE PHONE SCAMS

CUB's Guide to Fighting Robocalls is updated regularly to reflect the latest robocall news and scams. For this September update, we wanted to make consumers aware of four scams we've heard of recently. After reviewing these, continue reading the guide to learn more about robocalls and CUB's tips to stop them.

The scam: Voting misinformation.

This month, Attorney General Kwame Raoul warned Illinoisans about robocalls giving misinformation about voting by mail.

The lie:

An automated recording claimed that if you vote by mail your personal information will be shared with:

- The Centers for Disease Control and Prevention (to target people for mandatory vaccines);
- The police (to nab people with outstanding warrants); and
- Creditors (to locate people who owe debt).

The truth:

Attorney General Raoul said: "I am urging voters to be aware that Illinois law does not permit election authorities to share personal information, regardless of the voting method you choose." If you have questions about voting, please call the Illinois State Board of Elections: 217-782-4141 or 312-814-6465.

"Voting by mail is as secure and confidential as in-person voting, and it's the safest method of voting for those concerned about COVID-19 exposure," said State Board of Elections Executive Director Steve Sandvoss.

The scam: Electric rip-offs.

Several CUB staffers have reported getting robocalls offering a 30 percent savings on your electric bills.

The lie:

CUB General Counsel Julie Soderna reported getting three robocalls in two weeks that started the same way: "This is an apology call from your electric provider—you have been overcharged by a third-party electric supplier. Press 1 to get your refund and a 30 percent discount on your electric bill." Then a salesman comes on and tries to switch you to an alternative supplier.

The truth:

The salesman was pitching "Switch Energy" at a rate that was about 16 percent higher than the utility rate. This is typical of reports we get from consumers, and it's no surprise to us that such rip-offs have robbed Illinois consumers of more than $1 billion over the last five years. Don't press 1 for such calls. If you do sign up, call the alternative supplier listed on your bills to find out what you're paying, or call CUB to learn how to identify rip-offs.

The scam: Government imposters.

The robocall claims to be from the Social Security Administration or the Internal Revenue Service. To make the scam look "official," the imposter might have a fake name or number displayed on your caller ID.

The lie:

According to The Wall Street Journal, here's how the Social Security scam works: A prerecorded voice alerts you that you're the victim of stolen identity or a participant in a crime. To fix the matter, you need to call a number. If you call the number, the swindlers who take such calls will do anything they can to get your personal information or money. (Note: The Social Security Administration also warned about scams claiming that benefit payments may be suspended or decreased due to office closures related to the COVID-19 pandemic. The IRS reported scams related to stimulus checks and filing extensions.)

The truth:

The Federal Trade Commission says government agencies don't ask people to send money for unpaid loans, wire money or add money to a prepaid debit card. "I got three different robocalls from three different numbers, all claiming to be from Social Security," a Quincy woman wrote to the Better Business Bureau. "(The robocall) said there was a problem with fraudulent activity on my Social Security Number and asked me to call back. I knew it was a scam and didn't call back." If you ever have questions about a government agency, call the agency yourself.

The scam: Bogus COVID-19 test kit.

A robocall that targets people with concerns about diabetes and coronavirus. It's one of many taking advantage of the pandemic.

The lie:

A robocall reportedly says: "If you're a diabetic and using insulin, you can get a free diabetic monitor and testing kit for COVID-19. Press 1 for more info." Other telecom scams during the pandemic peddle phony COVID-19 cures and work-from-home schemes.

The truth:

Don't press 1. They just want your personal information. In general, don't engage, even if the recording instructs you to press a number to be removed from the call list. That might just signal to the robocaller that a live person has the number—and it may lead to more calls.

Guide to Fighting Robocalls

August 2020

The latest news on the robocall fight

Robocalls—prerecorded messages from computer-generated dialers—are such a pervasive nuisance that they are inflicting major damage to how we communicate. Illinoisans are bombarded with billions of these calls each year.

About 70 percent of Americans surveyed by Consumer Reports said they don't pick up the phone if they don't recognize the number. This means people miss reminders for doctor appointments or repair visits, charities are losing donations they've traditionally solicited by phone, and small businesses waste time calling contacts who don't answer.

While we push elected officials and telecom companies to end the pesky calls for good, this guide will give you the tools to reduce robocalls.

There has been some good news since CUB first released this guide in 2019: A new law, the TRACED Act, was passed to help combat robocalls, and telecom companies are implementing new technology to block them.

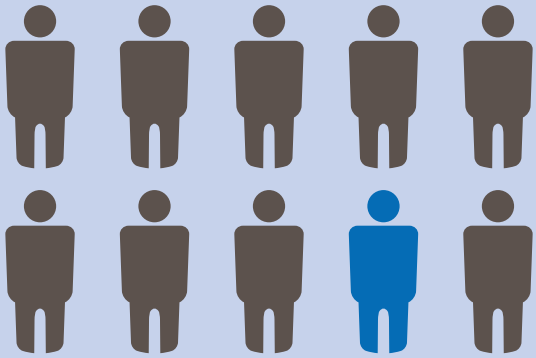
The law

At the end of 2019, the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act became federal law. The act extends the statute of limitations for law enforcement to go after bad actors and increases penalties. It also requires phone companies to validate calls before they reach you. If you get a call on your cellphone and Caller ID labels it "Scam Likely" that could be the result of your wireless provider using an authentication system. But a full, effective implementation of this service could take years.

Remember, with sales robocalls—prerecorded calls promoting goods or services—a telemarketer **must** first have your written consent, otherwise it's illegal.

But some prerecorded messages are legal, including:

- information-only calls, such as flight cancellations, appointment reminders or school closing announcements;
- calls from a business to collect a debt you owe;
- calls from or on behalf of politicians;
- calls from certain health care providers, such as a pharmacy informing you a prescription is ready;
- messages from banks, telephone carriers and charities, as long as those entities make the calls themselves.



One in 10 Americans are scammed each year, resulting in an annual loss of

$9.5 billion

Source: TechRepublic

The latest scams

If there's a two- or three-second delay when you pick up the phone, it's a recorded call. If you stay on the line, you might find one of these frauds on the other end.

Government scams: Some calls will try to convince you that you owe the Internal Revenue Service (IRS) money, cleverly using titles and numbers on your Caller ID that look like they're from the agency. Other calls purport to be from the Social Security Administration and claim an officer is on the way to your home with a warrant for your arrest. The recording then asks you to press 1 to talk to a real person.

Don't fall for it. If a government agency thinks you've done something wrong, it won't call. You will receive a letter detailing the issue.

Any calls offering to solve a legal problem by buying gift cards and sending them to a certain address are scams. Police and other government agencies do not accept gift cards to pay tickets or any other debt.

Benefits scams: Sometimes fraudsters will offer low credit card rates, ways to get money fast, or savings on health insurance. (These scams are especially prominent at the beginning and end of the year, when plans are ending and renewing.) The pitch may be as simple as "take advantage of the free programs available to you" and it may name-drop existing programs or businesses to appear legitimate.

Neighbor spoofing: A robocaller uses your area code and/or prefix to appear as if someone locally—maybe even a friend or neighbor—is trying to reach you.

"Say yes" scams: Have you answered an automated voice asking, "Can you hear me now?" If such a call lures you into saying "Yes," it can use the recording as proof that you gave permission to sign up for some type of costly offer you normally wouldn't buy.

Chinese Consulate scams: Many consumers, including staff members at CUB, have reported lengthy robocalls in Mandarin. Some ask you to meet at a consulate office to receive a package—but not before you make a payment or divulge personal banking information.

What NOT to do when you get a robocall

It's best NOT to answer a suspicious call. But if you do answer a sales robocall:

- DON'T stay on the line. Hang up immediately;
- DON'T try to call the number back to complain. That might lead to more calls;
- DON'T follow the call's instructions. If a robocall offers you the option of pressing a number to stop future calls, that might just be a trick to confirm that your number is "live" and ripe for more calls;
- DON'T say "yes." Beware of the "say yes" scam (see the description on this page).

Alternative supplier scams: CUB staffers have reported receiving robocalls asking consumers if they want to save 30 percent on their electric bills. But after being connected with a real person, we find that the rate offered is significantly higher than the electric utility's price.

5 steps to reducing robocalls

You won't completely avoid robocalls, but you can reduce the number you receive.

Step 1: Confirm you're on the Do Not Call List.

It's true, scammers get around the Federal Trade Commission's Do Not Call Registry, but it's still a good idea to join the list.

You will get fewer robocalls from companies that follow the law, so any sales calls you get are likely from a scammer. If your number is registered, you can report offending companies to help build a case against them.

You can register your home and cellphone numbers (or confirm those numbers are already on the list) here:

Call **1-888-382-1222** from the phone you want to register (TTY: **1-866-290-4236**) or register online at **DoNotCall.gov**. (You will receive a confirmation email that you must respond to within 72 hours to complete your registration, but you will only have to register your number once.)

Beware of any sales call that offers to put you on the Do Not Call List. Reader's Digest warns that "no company making a sales call has the power" to do that.

Step 2: Use voicemail as a weapon against robocalls.

One of the easiest ways to fight robocalls is to screen calls through your voicemail/answering machine. Telemarketers often hang up when the call goes to voicemail.

With a landline answering machine, if the caller is a friend, pick up the phone before he or she is done leaving a message. With a smartphone Caller ID, you can screen for friends and let everything else go to voicemail.

The CEO of one robocall-blocking service told USA Today that he advised his mom to simply turn off her ringer, send calls through an answering machine, and then monitor the messages.

Step 3: See what your phone can do for you.

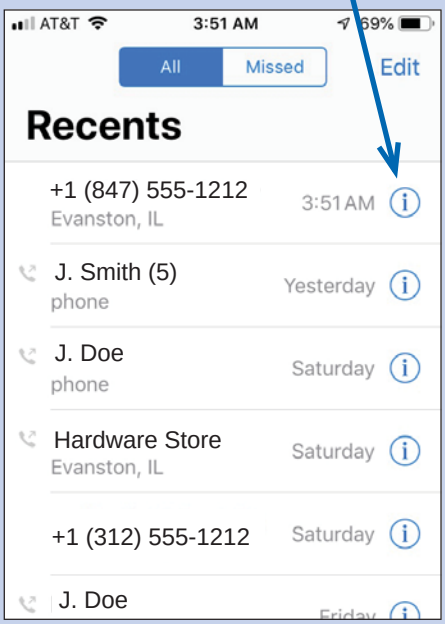
Spam-blocking protection: Your phone may have this functionality. Typically, here's how you check if it's activated.

- iPhone (iOS 13) users: Go to "Settings," and then "Phone." Select "Silence Unknown Callers."
- Android users: From the Phone screen, hit the three vertical dots at the top right. Tap "Settings." Choose "Caller ID & spam" or "Filter spam calls" to turn it on or off.

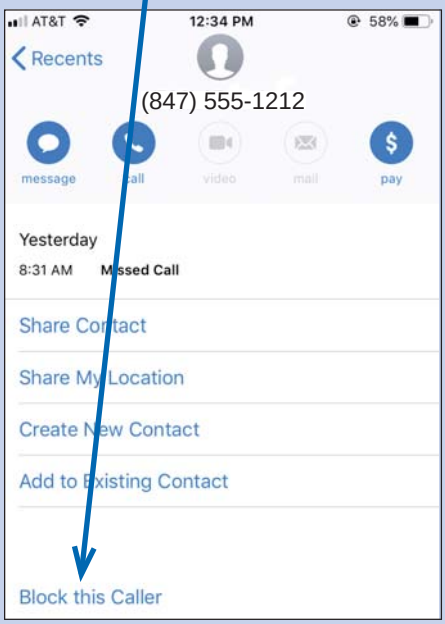
Your smartphone's number-blocking technology: If you get an unwanted telemarketing call, you can block that number for good. The directions below are general—steps may vary depending on the device. If you have additional questions, make sure to contact your phone's manufacturer.

Blocking calls on iPhones:

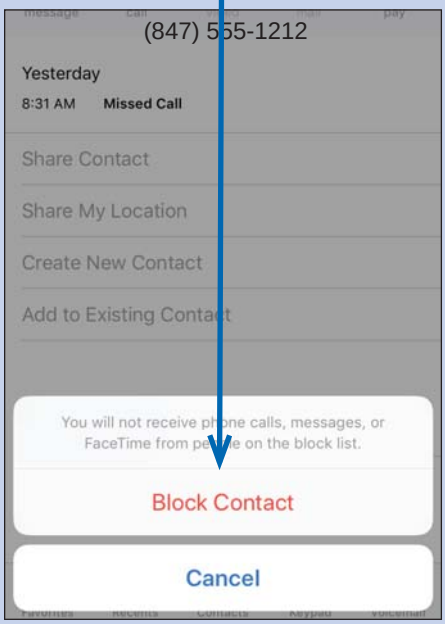
1) On your list of recent calls, tap the info icon (the encircled "i") next to the caller you want to block.



2) Choose to block this caller.

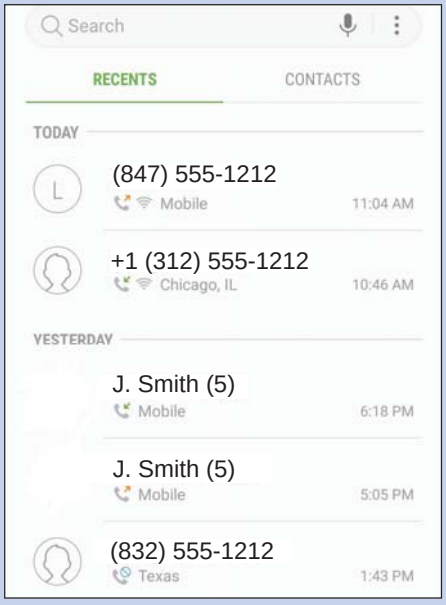


3) Confirm you want to block the contact.

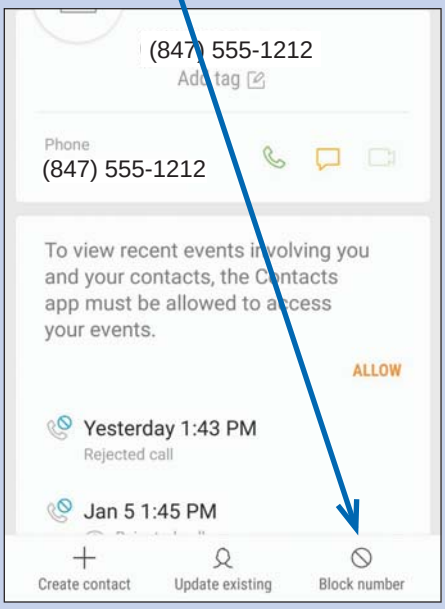


Blocking calls on Android phones:

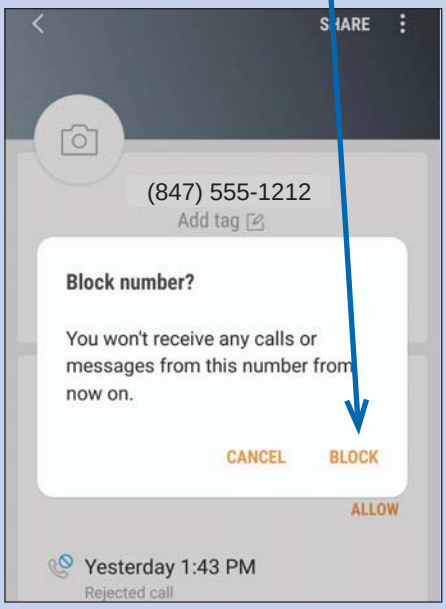
1) On your list of recent calls, tap on the caller's name and long-press the number.



2) Tap "Block number"



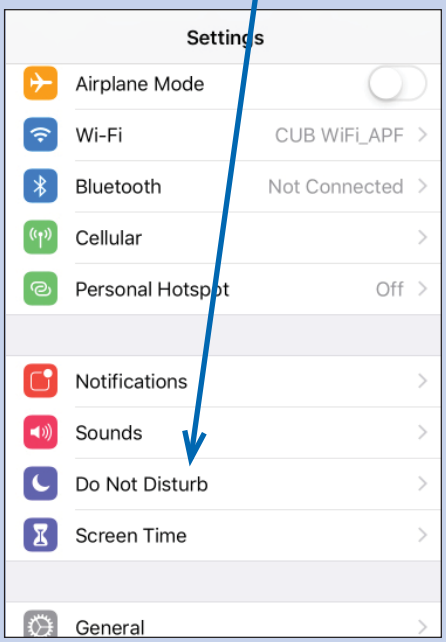
3) When asked to confirm, tap "block."



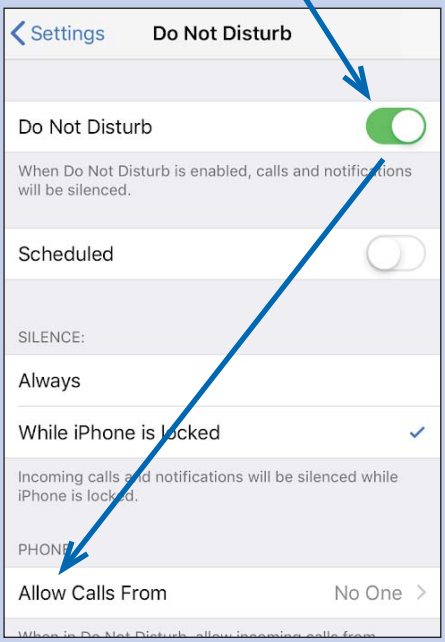
Try your smartphone's Do Not Disturb feature: This could be an effective solution for a lot of people. In this mode, your calls are sent directly to voicemail. You won't get notified, so you might miss some calls you want, but you can set it up so calls from people in your contacts list can ring. For more details go to **Support.Google.com** and search for "Limit interruptions with Do Not Disturb on Android." Or, visit **Support.apple.com** and search for "Use Do Not Disturb on your iPhone." The directions below are general—steps may vary depending on the device. If you have additional questions, make sure to contact your device's manufacturer.

Setting Do Not Disturb on iPhones:

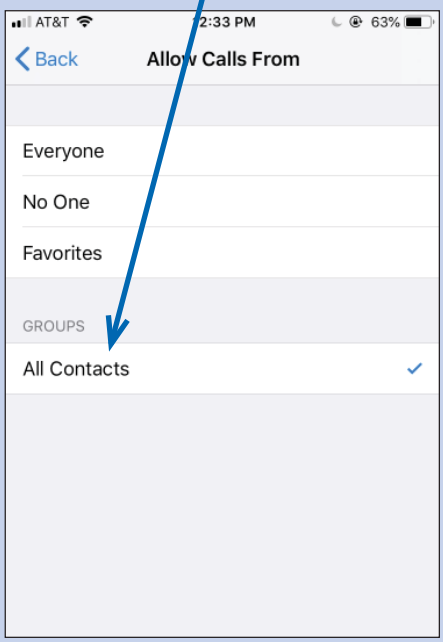
1) Go to Settings and choose "Do Not Disturb."



2) If the Do Not Disturb button is green, it's on. Then select "Allow Calls From."

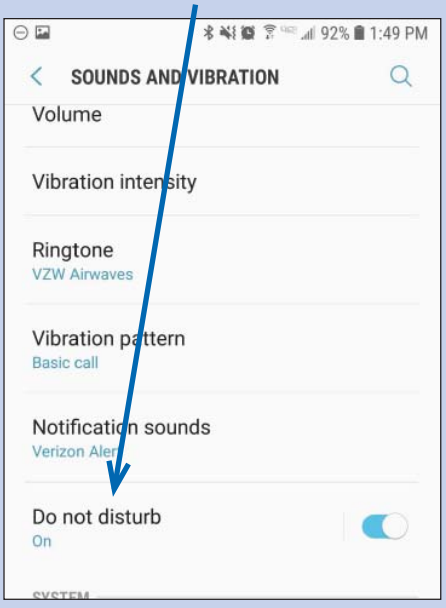


3) If you want to ignore all calls except those from your contacts list, choose "All Contacts."

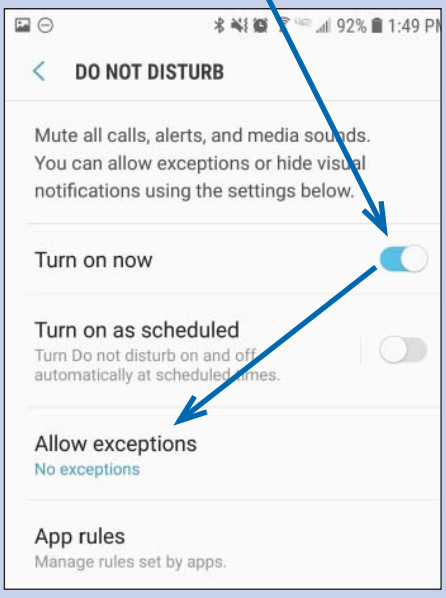


Setting Do Not Disturb on Android Phones:

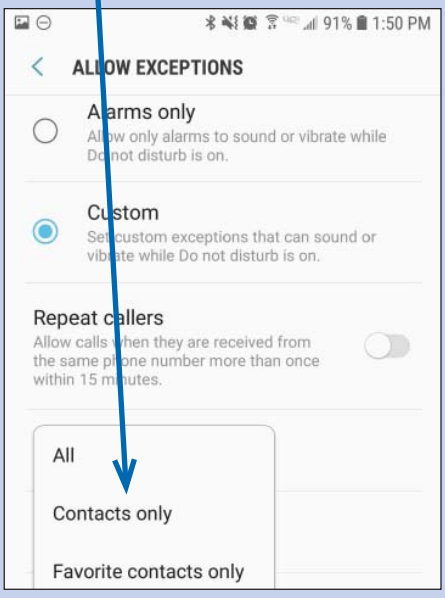
1) Go to Settings, choose "Sounds and Vibration" or "Sound and Notifications," and then "Do Not Disturb."



2) If the Do Not Disturb button is blue, it's on. Then select "Allow Exceptions."



3) To ignore all calls except from your contacts list, choose "Contacts Only."



Step 4: Ask your home phone company if it offers free services.

Call-blocking services from your digital home phone company: Internet home phone services—like Comcast Digital Phone Service and AT&T U-verse—offer free call-blocking features.

For example, AT&T offers "Digital Phone Call Protect." This free service automatically blocks calls from known spammers (they get a busy signal) and Caller ID tells you if other calls are suspected spammers.

These digital home phone providers also offer the effective robocall-blocking service Nomorobo for free. (Nomorobo also is available for smartphones. See the chart on page 6 for more information.)

AT&T U-verse: ATT.com (Search for "call blocking for digital phone."), **1-800-288-2020**

Comcast XFinity: XFinity.com (Search for "call screening."), **1-800-934-6489**

Call-blocking services from your wireless company: Your carrier offers robocall-blocking protection. CUB does not endorse telecom offers, but the chart below gives examples of what's available. Remember, these services may not be available on all devices. Always ask your carrier what kind of free anti-robocall services it offers.

Your wireless company's call-blocking services

Carrier	Plan	Price	Notes	For more info
AT&T	Call Protect	FREE (Advanced service, "Call Protect Plus," costs $3.99/month/line.)	Automatically sends callers not in your contact list to voicemail. Only available for HD Voice, iPhone 6 or newer, or AT&T Android phones. Prepaid accounts NOT eligible, and devices bought through companies other than AT&T may not be eligible.	**ATT.com** (Search "Block robocalls")
Sprint	Call Screener Basic	FREE (Advanced service, "Call Screener Plus," costs $2.99/month/line.)	Identifies unwanted malicious calls and allows users to block them and report potential fraudsters.	**Sprint.com** (Under "Plans" click "Add-on Services" and find Call Screener Plus. After a free trial period with the advanced service, you can choose the FREE basic service.)
T-Mobile	Scam ID, Scam Block, and Name ID	Scam ID and Scam Block are FREE for post-paid customers (those who get a bill for calls already made). But the company also offers an advanced service called Name ID for $4/month/line.	**Scam ID**: Alerts you immediately when you get a call from a likely scammer (free). **Scam Block**: Allows you to block likely scammers (free). **Name ID**: Identifies callers and allows you to block calls. You can send whole categories of calls (telemarketing, survey, political) directly to voicemail. ($4/month/line. Also, data charges may apply for Caller ID to work.)	**T-mobile.com** (Search for "blocking scams & unwanted calls.")
Verizon	Call Filter	FREE (Advanced service, "Call Filter Plus," costs $2.99/month/line.)	Warns you about potential spam, allows you to automatically block robocalls and report unsolicited numbers.	**VerizonWireless.com** (Search for "Call Filter")

Step 5: Check what third-party services are available.

Call-blocking devices for your traditional landline: Unfortunately, people with traditional copper landlines—those who could be targeted by scam artists—often have the fewest tools to fight robocalls. If you own a traditional landline, one option to reduce this nuisance is to buy a device that connects to the phone and blocks calls. Examples include Sentry 3.1., CPR Call Blocker and Digitone ProSeries Call Blocker. (A review on **Amazon.com** found several models ranging from about $50 to more than $100.)

Typically, these devices are based on a "blacklist" database of known spammers and a "whitelist" of numbers approved by you. Before you buy such a device, confirm it will work on your landline.

One concern to investigate: Will the device you're considering block legitimate calls in an emergency or good robocalls (a message from your pharmacy that a prescription is ready)? Also, some have complained that the set-up instructions are complicated. However, for people worried about a parent being victimized by a robo-scam, this could be a solution—just not a free solution.

Apps for your wireless phone: Applications, available in the App Store for iPhone or Google Play for Android, can help weed out robocalls and scam numbers. CUB does not endorse apps, but the chart below summarizes some of the available options.

Remember, not all apps are compatible with all devices. Also, while some apps are free to download and use, they may offer upgrades with more features at an extra cost. As with any app, read the privacy policy to find out what kind of information is collected.

Bonus tip: Robotexts

Robots aren't just calling your cellphone, but texting it too. More than 70 percent of all cellphone text spam is designed to defraud you in some way, according to a study by Cloudmark, a company that makes anti-spam software.

It is illegal to send commercial message to your wireless devices without your prior written consent, but noncommercial messages like political surveys or fundraising messages are allowed.

Just like robocalls or email spam, text message spam tries to get you to share personal information or click on a link to install malware on your phone.

Third-party apps

App	Price	Notes	For more info
Hiya: Spam Phone Call Blocker	Free	Identifies calls/texts you want, blocks the numbers you want to avoid.	**Hiya.com**
Nomorobo	Free for people who have Voice Over Internet Protocol (VoIP) lines—including AT&T U-verse and Comcast Digital Phone. For people with smartphones, $1.99 per month after a free 14-day trial.	Automatically blocks spam/scam robocalls, but allows good robocalls (school closings, prescriptions) to pass through. Winner of the FTC's Robocall Challenge in 2013.	**Nomorobo.com** (For a list of all the VoIP providers that offer Nomorobo, see Nomorobo.com/signup.)
RoboKiller	Free week trial then $3.99/month or $29.99/year membership.	Automatically blocks more than a million telemarketers and robocalls, even if they're trying to spoof or change their numbers. Winner of the FTC's Robocall Challenge in 2015.	**Robokiller.com**
Truecaller	Free with ads, but you have the option to purchase a premium package with no ads for $2.99/month or $26.99/year.	Identifies spam calls/texts and allows you to block them. Has a custom call-blocking feature that allows you to block other calls you don't want.	**Truecaller.com**

These unsolicited messages could slow your cellphone performance by taking up memory and depending on your phone plan, could lead to extra charges on your cellphone bill.

Many of the tips to reduce robocalls will work to reduce text spam as well. Some text-specific things to know are:

- Text messages that ask for personal information are scams. Legitimate companies don't ask for information like account numbers or passwords by email or text.
- Don't reply. While you may have requested to receive regular texts from your doctor or your favorite clothing store, beware of texts from unknown companies or companies that usually don't reach out to you that way. Don't reply to strange texts. Even if the message says you can opt out of future texts by replying STOP, your reply may just let scammers know that the number is actively in use. No matter how annoyed you are, engaging is likely to make the problem worse. ven if the message says you can opt out of future texts by replying STOP, your reply just lets scammers know that the number is actively in use. No matter how annoyed you are, engaging is almost guaranteed to make the problem worse.
- Don't click on links in the message. Links can install malware on your phone or take you to fake sites that look real but whose purpose is to steal your information.
- Forward the texts to 7726 (SPAM). This works for AT&T, Verizon Wireless, T-Mobile, and Sprint and tells those wireless companies to block future texts from those numbers.
- Review your cellphone bill for unauthorized charges and report them to your carrier.

Filing a complaint with the FTC

If you get harassed by robocalls, file a complaint with the Federal Trade Commission (FTC) by visiting **FTC.gov/complaint** and click on the FTC Complaint Assistant icon, or calling **1-877-FTC-HELP**.

You will be asked a series of questions. The more information you can provide, the better chance you have at getting a response and action being taken. Have the following information readily available:

- Contact information (your name, phone number, email).
- Name and number of the company or person calling you.
- Information related to the call, such as what the robocaller said to you.

Sources for this guide

You can find links to all sources CUB used to write this guide on our WatchBlog:

https://www.citizensutilityboard.org/blog/2020/02/12/robocall-guide-sources/