# If You Hear This 4-Word Phrase When You Pick Up the Phone, Hang Up Immediately

If you've been getting more robocalls lately, you are not alone. Phone call scams have increased a whopping 118% in the past year, according to First Orion, and millions of Americans have fallen victim to phone scammers looking to steal their money and identities.

Hopefully, you've already learned not to answer calls from these area codes and know how to tell if the "iPhone virus warning" is a scam. But now there's another common phone scam trick to watch out for. Experts are warning about a robocall that starts with the simple four-word phrase "Can you hear me?" in hopes of recording your response and using it to commit fraud.

Keeping these iPhone privacy settings up to date can boost your smartphone security and privacy, but they might not protect you in this case. Luckily, we've got the scoop from experts on why this phone scam is so dangerous, what you should do if you respond and how to avoid falling victim in the future.

## Why this phone scam is so dangerous

In general, all phone scams "are designed to do two things: gain information about you that can be used to impersonate you [through] identity theft, and get you to give money to the scammer," says Adam Gordon, an instructor at ITProTV, which provides professional IT training.

In this particular phone scam, a recorded voice will ask, "Can you hear me?" when a victim answers the call. The phrase is designed to trick the victim into responding "yes," while the person or computer on the other end is recording. From there, the scammer can use the recording to access important online accounts, make purchases and commit fraud like identity theft. All they have to do is play the recording of your voice saying "yes" when asked to authorize a log-in or agree to a major purchase.

"This phone scam is particularly frightening [because] they simply rely on the human behavior of answering a quick question," says Matthew Shirley, director of offensive cybersecurity operations at Fortalice, a cybersecurity services company.

By getting right to the point, the scammer catches victims off guard and forces them to act fast before they have the chance to think rationally. Scams on Uber and Facebook Marketplace also rely on this strategy, so it's important stay vigilant across the board.

## The danger of chatbots and AI

This phone scam also reveals the sneaky potential of new chatbots and artificial intelligence (AI) technology to imitate human speech. These days, "AI chatbots are so advanced that they give the 'human touch,' being able to masquerade as a human successfully in many cases, and can be indistinguishable from a human in situations like a phone call," Gordon says.

Unfortunately, scammers are now using this new technology to fool victims into believing they are speaking with a real person on the phone. In a new version of the "Can you hear me?" phone scam, the call begins with a human-like voice saying "Sorry, I'm having issues with my headset."

This tactic makes people think that a real person is on the other line. It also "gives a little room for interpretation of pacing," like odd delays, which would ordinarily tip off the victims that they might be dealing with a phone scam, Shirley says.

## What your voice saying "yes" can unlock

With the recording of the victim's affirmation, scammers can access sensitive information, authorize payments or sign up for services that the victim doesn't want. "Just think about what someone with a recording of you saying 'yes' can attempt to access, unlock, change or authorize in today's remote-centric and faceless world," Gordon says. If the scammer is asked to agree to a purchase or

service, for example, they will simply play the recording of your voice saying "yes."

That's why it is so important to protect your online accounts by creating strong, unique passwords and using two-factor authentication when you can. At the end of the day, it's much easier to protect yourself from scammers than it is to recover a hacked Facebook account or hacked Instagram account.

## Other robocall scams to watch out for

Using realistic chatbots and AI is one of the most popular tricks scammers use to hack your stuff. In fact, robocalls made up 60% of all scam phone calls in 2021.

"Robocalls are incredibly cheap, costing only handfuls of dollars to send millions of calls. This leads to a surplus of scam call opportunities," Shirley says. Scammers may also use chatbots to contact you by text message, so learning how to stop spam texts can block scams from reaching your messages app too.

In one frequent phone scam, a recorded voice will tell the victim that their car warranty is about to expire unless they take immediate action by calling a phone number, sharing information or sending money.

Other robocall scams may try to persuade victims to make a donation, invest in a business or sign up for a free trial, loan, lottery or vacation timeshare by handing over their credit card or bank information.

## How to guard against these types of scams

To avoid falling victim to this phone scam and other robocall scams, it's best to never answer calls from unfamiliar phone numbers, or quickly hang up if you do. Pressing any numbers or responding to the caller confirms that the phone number is active, which might lead to more robocalls, Gordon says.

Be cautious when speaking with any unknown caller too. "Under no circumstances should you hastily respond to their questions or give anything that is requested," Shirley says. "Assume that any unknown party attempting to solicit payment or information may not be who they claim to be."

Finally, both Gordon and Shirley suggest signing up for the National Do Not Call Registry and using a call blocking or labeling app to screen and block unknown calls. With these apps, each caller will receive short prompts to verify their identity before the call is forwarded to your phone. Many phone carriers also provide security apps and services to block unwanted calls.

## What to do if you responded to the scammer

Already said "yes" in response to this phone scam? Start securing your online accounts and important information now. "The sooner you act, the better," Gordon says.

If a scammer has authorized a purchase under your name, Gordon recommends contacting the company through which the payment was made—whether that's a credit card company, bank, money transfer app, wiring company like Western Union or a gift card/prepaid card/cash reload card company—and telling them what happened. These companies might be able to stop the payment or issue a refund.

You should also change your passwords to sensitive accounts and monitor your credit report for unusual activity. If you think a scammer might have remote access to your computer, update your computer's security software and look for the signs that your computer has been hacked.

## How to report phone scams

If you receive a call that appears to be a phone scam, Gordon suggests reporting it to the Federal Trade Commission (FTC) at ReportFraud.ftc.gov. Make sure to

share the number that appears on your caller ID and any number you are told to call back. The FTC uses this data to identify, label and block illegal callers, Gordon says. Of course, learning how to stop robocalls and spam calls for good can help you avoid receiving these calls in the first place.

**Sources:**

- Adam Gordon, edutainer at ITProTV
- Matthew Shirley, director of offensive cybersecurity operations at Fortalice
- First Orion: "2021 Scam Call Trends"
- MalwareBytes Labs: "More than a quarter of Americans fell for robocall scam calls in past year"

# BBB Scam Alert: If caller asks “Can you hear me?,” just hang up

By Better Business Bureau. October 21, 2020.

The Better Business Bureau is warning consumers about an old scam with a new twist. The “Can You Hear Me?” scam has long been used to coerce businesses into purchasing office supplies and directory ads they never actually ordered, but now it’s targeting individual consumers, as also targeting individual consumers.

For the last few days of January, more than half of the reports to BBB Scam Tracker have been about this one scam. Consumers say the calls are about vacation packages, cruises, warranties, and other big-ticket items. So far, none have reported money loss, but it’s unclear how the scams will play out over time or if the targets will be victimized later.

Here’s how it works: You get a call from someone who almost immediately asks, “Can you hear me?” Their goal is to get you to answer “Yes,” which most people would do instinctively in that situation. There may be some fumbling around; the person may even say something like, “I’m having trouble with my headset.” But in fact, the “person” may be a robocall recording your conversation… and that “Yes” answer you gave can later be edited to make it sound like you authorized a major purchase.

**BBB is offering consumers the following advice:**

- Use Caller ID to screen calls, and consider not answering unfamiliar numbers. They will leave a message if it's important, and you can call back.
- If someone calls and asks, “Can you hear me?” do NOT answer “Yes.” Just hang up. Scammers change their tactics as the public catches on, so be alert for other questions designed to solicit a simple “yes” answer.
- Make a note of the number and report it to BBB.org/ScamTracker to help warn others. BBB also shares Scam Tracker information with government and law enforcement agencies, so every piece of information helps track down scammers.
- Consider joining the Do Not Call Registry (DoNotCall.gov) to cut down on telemarketing and sales calls. This may not help scammers since they don’t bother to pay attention to the law, but you’ll get fewer calls overall. That may help you more quickly notice the ones that could be fraudulent.

- Check your bank and credit card statements regularly for unauthorized charges. Checking your telephone and cell phone bills is also a good idea. Scammers may use your voice's “Yes” recording to authorize charges on your phone. This is called “cramming,” and it’s illegal.

**For more information**

Report scams to BBB Scam Tracker (BBB.org/ScamTracker).

Check out BBB.org to look up a business, file a complaint, write a customer review, report a scam, read tips, follow us on social media, and more!

- Better Business Bureau: "BBB Warning: If caller asks 'Can you hear me?,' hang up"

The post If You Hear This 4-Word Phrase When You Pick Up the Phone, Hang Up Immediately appeared first on Reader's Digest.