SCAMS & FRAUD

Why You Shouldn't Answer Calls From Unknown Numbers

Avoid scams — including the 'say yes' or 'can you hear me' scam – by ignoring unsolicited callers

By Matt Alderton, AARP | 8 Comments
Published July 08, 2024 • EN ESPAÑOL

PHOTO COLLAGE: AARP (SOURCE: SHUTTERSTOCK; GETTY IMAGES)

If you watched television in the early aughts, you probably remember the iconic commercials from Verizon Wireless where a roving cellphone spokesman offered up a simple yet sticky catchphrase: "Can you hear me now?"

Some 20 years later, callers are still asking folks on the other end of the line if they can hear them. But now it's often scammers doing the asking, according to the Federal Communications Commission (FCC), which has warned consumers about so-called "can you hear me" scams — also known as "say yes" scams.

How it works: A criminal calls someone and asks a straightforward question like, "Can you hear me?" or, "Is this so-and-so?" in order to record the person saying "yes." In theory, the scammer can later use the recording for nefarious purposes.

Sometimes, the call ends immediately and abruptly. Other times, it's transferred to a live person who continues the conversation in an attempt to extract personal information that they can use for identity theft. In that case, the scammer may impersonate a bank employee, mortgage lender or utility company "to establish a legitimate reason for trying to reach the consumer," the FCC says. The main objective, however, is to obtain a recorded "yes."

Older adults are prime targets because they were raised to answer the phone, says Michael Bruemmer, vice president and head of global data breach resolution and consumer protection at consumer credit reporting company Experian. "They're preying on older people — people 55 and up — because we are so comfortable using the phone. Scammers take advantage of the fact that we will pick up a phone call because that's what our mom and dad or guardians told us to do."

What scammers can do with your 'yes'

Experts' views on this vary. Amy Nofziger, AARP's director of fraud victim support at the AARP Fraud Watch Network Helpline, says criminals can't do much with your "yes." When the FCC issued its initial consumer alert about "can you hear me" scams in 2017, it was believed that scammers could potentially use a consumer's recorded "yes" as a voice signature — a verbal agreement that could be played back on calls with banks or other service providers to authorize fraudulent charges by telephone. Thanks to multifactor authentication and other security measures, however, that's no longer a plausible scenario.

"Scammers can find way easier ways to steal from you than recording your two-second 'yes' and then hooking that up to a sales call and proving you agreed to it," explains Nofziger, who says criminals typically still need account numbers and other personal information to access one's accounts. And if they have those, they probably don't need a voice signature. The AARP Fraud Watch Network has "yet to hear of any money lost to a scam where a person says 'yes' and then the criminals use that recording to prove they bought something," she adds.

The Better Business Bureau (BBB) hasn't registered any monetary losses, either. Nevertheless, it wants consumers to be aware — just in case. "Many people have reported getting the calls, but they haven't reported anything bad happening afterwards," says BBB national spokesperson Melanie McGovern. "We've had no reports of anybody losing any money ... but just knowing that it's a possibility is why we're raising the red flag."

Even if they can't use a "yes" to access accounts or approve fraudulent charges, scammers might be able to use it for other purposes. "They use this 'yes' scam to check if the phone number is valid. If the phone number is valid, the phone will be a target for more scams," says Ping Yang, a professor of computer science at Binghamton University, State University of New York, where she also is director of the Center for Information Assurance and Cybersecurity. "They may also record your voice ... so they can do voice cloning in the future."

AI advancements may increase the threat

The danger may lie in more accessible and quickly advancing artificial intelligence tools, says Abhishek Karnik, head of threat research at the online security company McAfee. "Generating a voice clone has become increasingly easy. Therefore, social engineering attacks related to voice cloning have become a lot more realistic," explains Karnik, who says research by McAfee has found that modern tools can replicate how a person speaks with up to 95 percent accuracy, which makes it extremely difficult to tell the difference between real voices and fake ones.

Let it ring

Because fraud in general is rampant these days, it's wise to avoid responding to any unsolicited call. Once scammers get you on the phone, they can play with your emotions (instilling fear or anxiety, for example) to prevent you from thinking clearly, leaving you vulnerable to fraud. If the unknown caller is legitimate — someone from your doctor's office, for instance — he or she will leave a message. A scammer will move on to another potential victim.

Combined with personal information gleaned from your social media accounts or the dark web, a voice clone generated from just three to four seconds of audio during a "can you hear me" call could be used to impersonate you on the phone (using a spoofed number) to a friend or loved one, making it easy for criminals to scam money from them by convincing them that you're in need of emergency assistance (as in a grandparent scam). Karnik adds, "If you have the voice and you can spoof a phone number, that really opens you up to very targeted sorts of scams that are extremely advanced at this point," he says.

How to protect yourself from 'can you hear me' and other scams

1. **Don't answer unsolicited calls.** "The easiest thing to do is don't answer your phone," Bruemmer says. Anybody that's not in your contact list should automatically go to voicemail. If it's important, the caller will probably leave a message or call back again.
2. **Let the caller speak first.** "If you do pick up the phone, always let the other person speak first. Don't even say, 'hello,'" suggests Bruemmer, who says most scammers use an auto dialer — an automated system that calls a bunch of random numbers at the same time and connects to a live person when someone answers the phone. "You can tell just by waiting. You can hear a click and a pause. That means you're on some sort of auto dialer. It could be legitimate — let's say a window replacement salesman — but more often than not it's not a good thing. And you probably don't need to listen to the window salesman anyway."
3. **Change your voicemail greeting.** Scammers who are after your voice might be able to get it by listening to your voicemail greeting. For that reason, consider using the default greeting that comes with your voicemail instead of recording one yourself.
4. **Be careful on social media.** Check your privacy settings and be mindful of what you post, Karnik cautions. A scammer who clones your voice probably will only be able to use it successfully if they have other personal information about you.
5. **Monitor your accounts.** If you think you've said "yes" to a "can you hear me" scammer, don't panic. "Take a look at your bank account, credit card statements and credit report to make sure there's no unusual activity," McGovern advises. "Those are things everybody can do all of the time."
6. **Report it.** Report scams to the FBI's Internet Crime Complaint Center (IC3) at ic3.gov, and the BBB at bbb.org/scamtracker. "If you get a suspicious call, it's really important to keep note of the number and report it to us," notes McGovern, who says reports help the BBB track trends and protect other consumers who are being targeted by the same scams.

Matt Alderton is a contributing writer who specializes in health and wellness, travel and technology. His work has also appeared in USA Today, Forbes *and* The Washington Post.