A wild one here. Scammers have figured out how to trick people using Siri, Alexa, and Google Assistant. Multiple reports claim they've been scammed when asking a voice assistant to call a customer service number. The BBB and FBI are warning people about the scam and I'm looking at how to avoid it.

TRT 135
STD OUT

SUPER

0-8 Jamey Tucker/whatthetech.tv

ON-CAMERA TEASE:
are scammers using Siri and Alexa to trick us out of our money? I'M JAMEY TUCKER, COMING UP WITH A WILD SCAM AND HOW TO AVOID IT.

ANCHOR INTRO

VOICE ASSISTANTS SUCH AS SIRI AND ALEXA CAN BE A BIG HELP THROUGH THE DAY, ANSWERING QUESTIONS, PLAYING MUSIC, AND GIVING WEATHER INFORMATION.

AND NOW, THERE ARE CLAIMS THESE ASSISTANTS ARE HELPING SCAMMERS TAKE MONEY FROM UNSUSPECTING USERS. OUR CONSUMER TECHNOLOGY REPORTER JAMEY TUCKER EXPLAINS.

PACKAGE SCRIPT

In terms of scams, this is a wild one. It involves fake phone numbers, fake companies, web searches, and Siri. Here's how the scam reportedly works: When someone asks Siri to call a number, like customer service, scammers trick them into dialing a fake number instead. The number of the scammer.
"Siri, call United Airlines"
An alleged victim reported to the Better Business Bureau when they asked Siri to call United Airlines, someone answered. It wasn't the airlines but an agent pretending to be with United asking for $125 to cancel a flight.
Another alleged victim said they asked Siri to contact Roku about setting up the device. Instead, someone pretending to be from Roku charged an $80 activation fee. So how do the scammers pull this off? They set up fake customer service numbers and promoted them to the top of search results. So when a voice assistant searches the web for a number, they deliver the top search result: the fake number.
Protect yourself by #1, don't trust a voice assistant to get it right.#2, don't assume when you search the web for a phone number that the first result is the legitimate company. #3 Don't be quick to give anyone a credit card number or personal information over the phone. Never use a debit card. It's easier to dispute a charge when using a credit card or PayPal.

I tried replicating this by asking all of the voice assistants to look up customer support numbers for the major airlines but did not get the fake websites the BBB says to be aware of because it does happen. That's What the Tech? I'm Jamey Tucker

ANCHOR TAG

AND IF YOU EVER SUSPECT YOU'RE THE VICTIM OF A SCAM REPORT IT TO THE BETTER BUSINESS BUREAU AND THE F.C.C.

WEB STORY

As scams go, this is a wild one.

The Better Business Bureau and FBI agencies are warning consumers about scammers using Siri, Alexa, and Google Assistant to trick people into giving them their money over the phone.

Here's how the scam reportedly works:

When someone asks one of these assistants to call a number, like customer service, scammers trick them into dialing a fake number instead.

An alleged victim reported to the Better Business Bureau when they asked Siri to call United Airlines, someone answered but it wasn't the airlines but an agent pretending to be with United. They asked for $125 to cancel a flight.

Another alleged victim said they asked a voice assistant to contact Roku about setting up the device. Instead, someone pretending to be from Roku charged an $80 activation fee.
There is no activation fee for Roku devices. This is a frequent scam when people first set up a Roku device. Someone pretending to be from Roku call or email and say an activation fee is required. Roku services are free and no activation is necessary.

So how do the scammers pull this off? They set up fake customer service numbers and promoted them to the top of search results. So when a voice assistant searches the web for a number, they deliver the top search result: the fake number. The scammer then tries to separate you from your money.

Protect yourself with these three steps:

- Don't trust a voice assistant to get it right. Siri, Alexa, and Google Assistant search the web for phone numbers. They won't verify it's the right one.
- Don't assume when you search the web for a phone number that the first result is the legitimate company. Scammers often bump fake sites and numbers to the top of the results. Instead, use the company's official app to contact support. Or, verify yourself that the website you're visiting is the site of the real company.

- Don't be quick to give anyone a credit card number or personal information over the phone. Never use a debit card. It's easier to dispute a charge when using a credit card or PayPal.

I tried to replicate this scam myself by asking all of the voice assistants to dial the numbers of customer support for all of the major airlines as well as cellular companies and Roku. Siri and Google Assistant returned the legitimate websites for United, Southwest, Delta Airlines, AT&T, Verizon, and T-Mobile.

When I asked the assistants to look up the websites for customer support, Siri and Google Assistant returned a third-party support page for Roku with phone numbers listed for customer service.

The BBB warning came out a few days ago and a field office for the FBI brought attention to it. However, the original warning from the BBB was actually released in 2019.