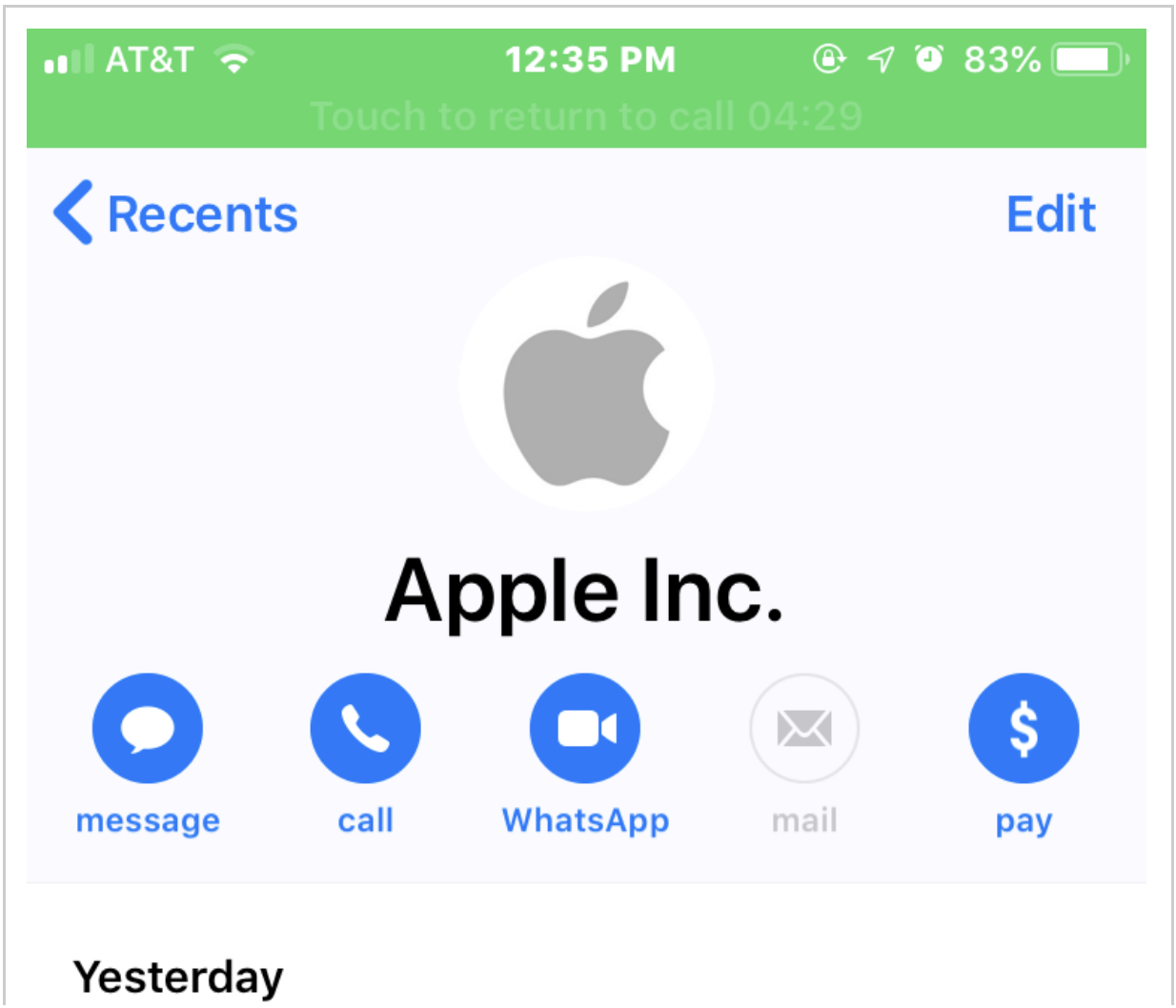
Apple Phone Phishing Scams Getting Better

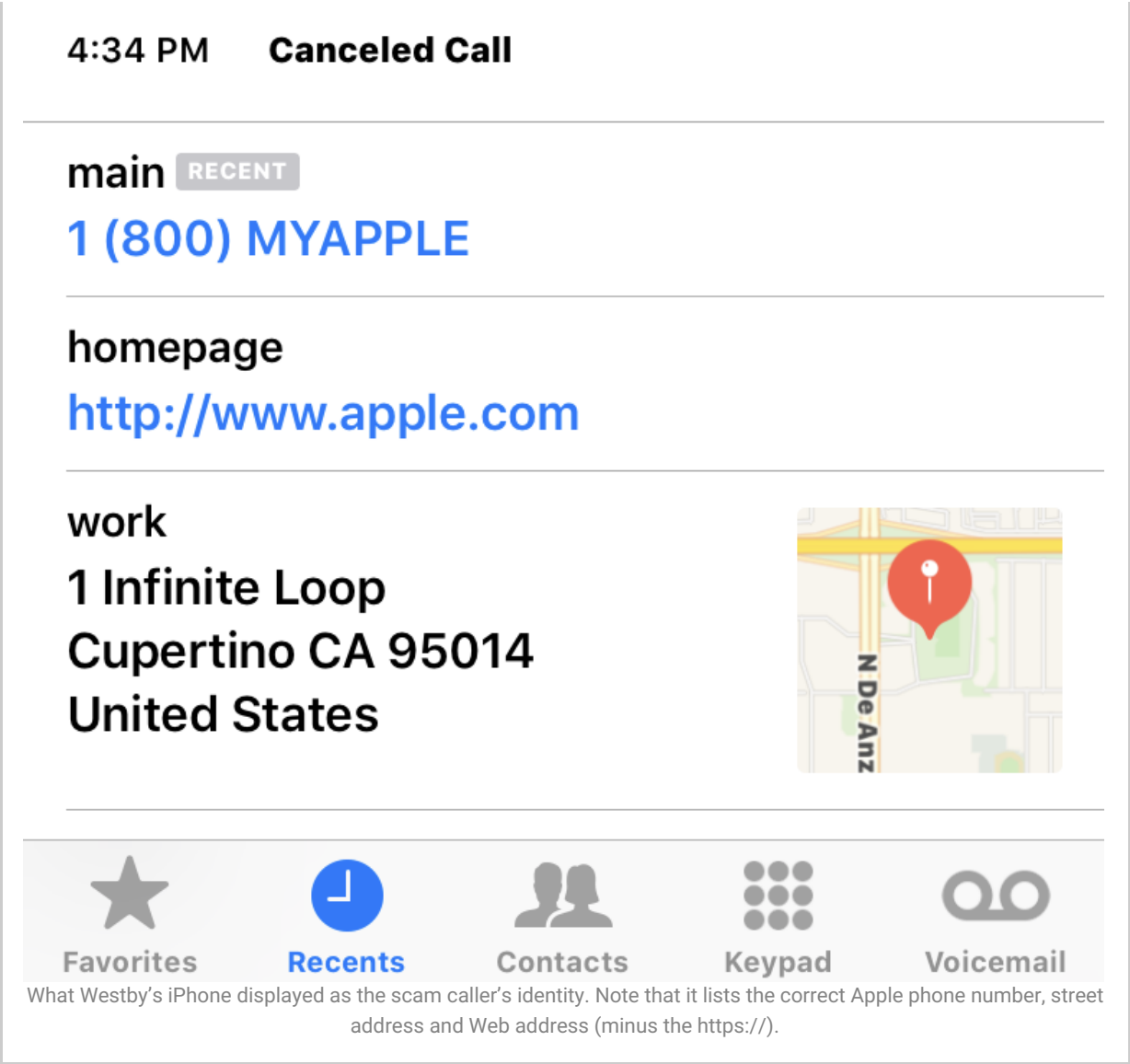
krebsonsecurity.com/2019/01/apple-phone-phishing-scams-getting-better

A new phone-based phishing scam that spoofs **Apple Inc.** is likely to fool quite a few people. It starts with an automated call that display's Apple's logo, address and real phone number, warning about a data breach at the company. The scary part is that if the recipient is an iPhone user who then requests a call back from Apple's legitimate customer support Web page, the fake call gets indexed in the iPhone's "recent calls" list as a previous call from the legitimate Apple Support line.

Jody Westby is the CEO of Global Cyber Risk LLC, a security consulting firm based in Washington, D.C. Westby said earlier today she received an automated call on her iPhone warning that multiple servers containing Apple user IDs had been compromised (the same scammers had called her at 4:34 p.m. the day before, but she didn't answer that call). The message said she needed to call a 1-866 number before doing anything else with her phone.

Here's what her iPhone displayed about the identity of the caller when they first tried her number at 4:34 p.m. on Jan. 2, 2019:



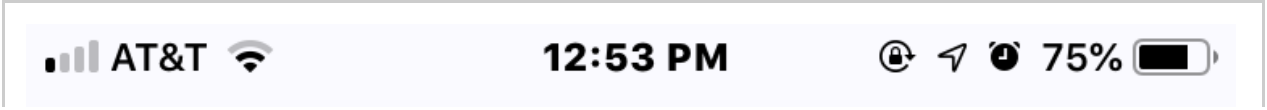


What Westby's iPhone displayed as the scam caller's identity. Note that it lists the correct Apple phone number, street address and Web address (minus the https://).

Note in the above screen shot that it lists Apple's actual street address, their real customer support number, and the real Apple.com domain (albeit without the "s" at the end of "http://"). The same caller ID information showed up when she answered the scammers' call this morning.

Westby said she immediately went to the Apple.com support page (https://www.support.apple.com) and requested to have a customer support person call her back. The page displayed a "case ID" to track her inquiry, and just a few minutes later someone from the real Apple Inc. called her and referenced that case ID number at the start of the call.

Westby said the Apple agent told her that Apple had not contacted her, that the call was almost certainly a scam, and that Apple would never do that — all of which she already knew. But when Westby looked at her iPhone's recent calls list, she saw the legitimate call from Apple had been lumped together with the scam call that spoofed Apple:



Recents Edit

Apple Inc.

message call WhatsApp mail pay

Today

11:51 AM	**Canceled Call**	
11:47 AM	**Incoming Call**	5 minutes
11:44 AM	**Incoming Call**	44 seconds

main RECENT

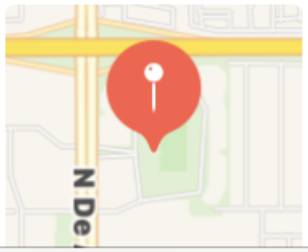
1 (800) MYAPPLE

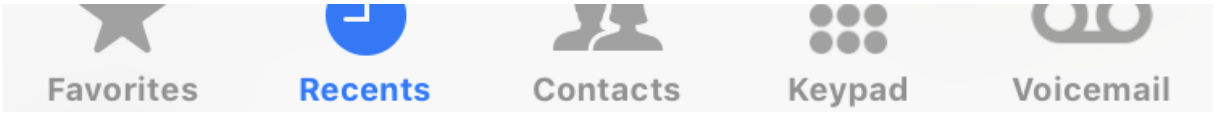
homepage

http://www.apple.com

work

1 Infinite Loop
Cupertino CA 95014
United States





The fake call spoofing Apple — at 11:44 a.m. — was lumped in the same recent calls list as the legitimate call from Apple. The call at 11:47 was the legitimate call from Apple. The call listed at 11:51 a.m. was the result of Westby accidentally returning the call from the scammers, which she immediately disconnected.

The call listed at 11:51 a.m. *was the result of Westby accidentally returning the call from the scammers*, which she immediately disconnected.

"I told the Apple representative that they ought to be telling people about this, and he said that was a good point," Westby said. "This was so convincing I'd think a lot of other people will be falling for it."

KrebsOnSecurity called the number that the scam message asked Westby to contact (866-277-7794). An automated system answered and said I'd reached Apple Support, and that my expected wait time was about one minute and thirty seconds. About a minute later, a man with an Indian accent answered and inquired as to the reason for my call.

Playing the part of someone who had received the scam call, I told him I'd been alerted about a breach at Apple and that I needed to call this number. After asking me to hold for a brief moment, our call was disconnected.

No doubt this is just another scheme to separate the unwary from their personal and financial details, and to extract some kind of payment (for supposed tech support services or some such). But it is remarkable that Apple's own devices (or AT&T, which sold her the phone) can't tell the difference between a call from Apple and someone trying to spoof Apple.

As I noted in my October 2018 piece, Voice Phishing Scams are Getting More Clever, phone phishing usually invokes an element of urgency in a bid to get people to let their guard down. If a call has you worried that there might be something wrong and you wish to call them back, don't call the number offered to you by the caller. If you want to reach your bank, for example, call the number on the back of your card. If it's another company you do business with, go to the company's Web site and look up their main customer support number.

Relying on anything other than a number obtained directly from the company in question — such as a number obtained from a direct search on Google or another search engine — is also extremely risky. In many cases, the scammers are polluting top search engine results with phony 800-numbers for customer support lines that lead directly to fraudsters.

These days, scam calls happen on my mobile so often that I almost never answer my phone unless it appears to come from someone in my contacts list. But as this scam shows, even that's not always a great strategy.

It's a good idea to advise your friends and loved ones to ignore calls unless they appear to come from a friend or family member, and most importantly *to just hang up the moment the caller starts asking for personal information.*

Apple has not yet responded to requests for comment.

Tags: 866-277-7794, apple phone phishing, Global Cyber Risk LLC, Jody Westby