This 'tech support' scam is stealing million from seniors, including my mom

My 76-year old mom is an incredibly tech-savvy senior who commands her gadgets more like a Millennial than someone born the same year the ballpoint pen was invented. She also has an array of built-in tech support experts all around her — including me — her own daughter!

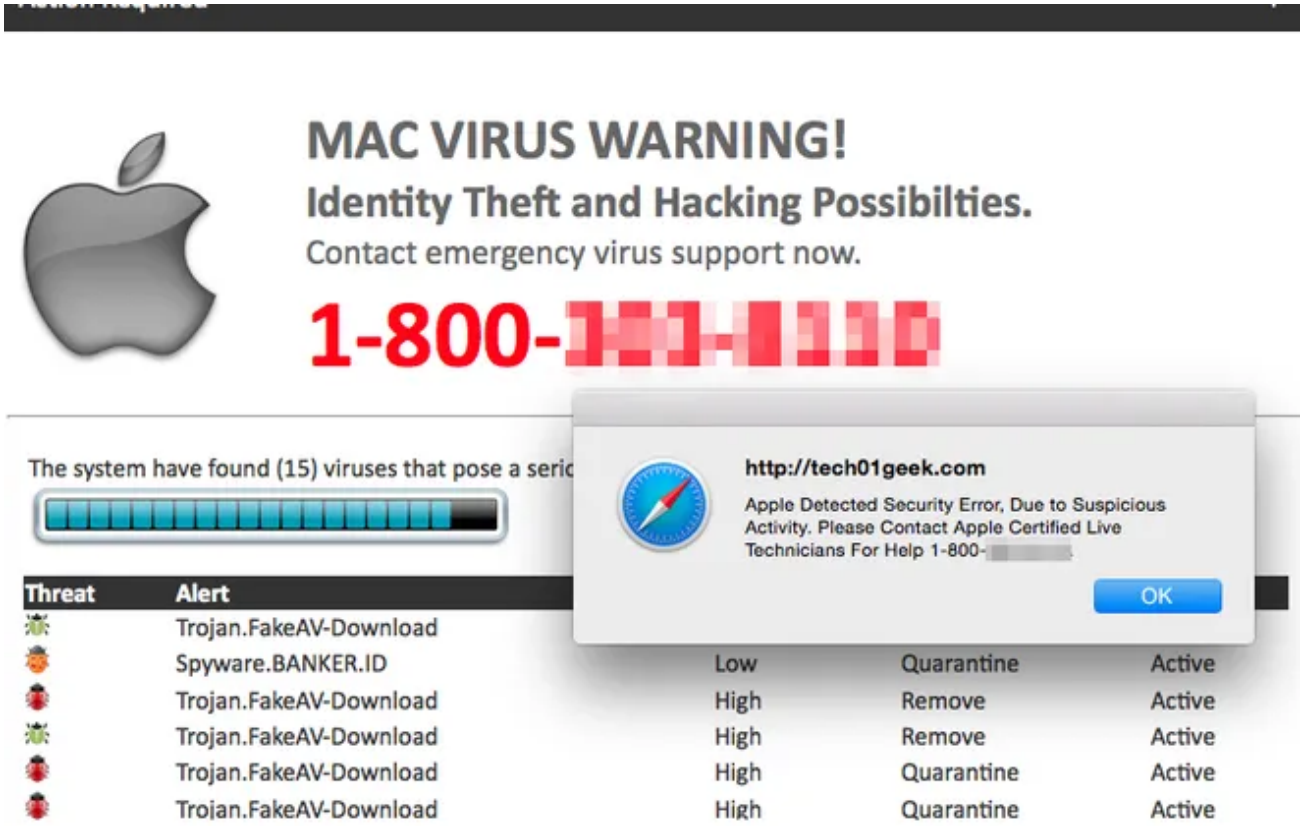
Still, when a giant yellow "alert" covered half of her MacBook Pro screen a few weeks ago, warning her that hackers had taken control of her device and to call the "Apple Support" number on the screen immediately or else...she did just that. But the real danger wasn't a virus on her computer, it was the man who answered on the other end of the phone.

A new version of the old tech support scam

"I'm so embarrassed," she tells me through tears. "There was a cursor running amok on my screen. I tried to grab it, and when I couldn't, I figured since it was happening on a Mac, it was real. I called the number on the screen, a man answered, "Apple Support," she pauses and her voice cracks again. "You know, these people are very good at what they do."

My mom lost $2,000 and even though she reported it to her bank right away, she's been told there's nothing they can do (more on this below). She feels horrible about it. I keep telling her not to feel bad. She's the victim of the most successful online fraud against seniors in America

today — a new version of the "tech support" scam — that's bilked people out of billions of dollars for the last several years.



Social media: Facebook's new tool lets users control what they see, share on their News Feeds

Beware this scam: Roku setup, activation scam doesn't include cold calls, bogus links

What's new is how scammers are targeting more people over the age of 60 online than by phone, according to an October 2020 report from the Federal Trade Commission. This coincides with the pandemic and more people of all ages spending more time in the digital world. The FTC also reports fraud losses totaled $388 million through the third quarter of 2020, a number that's up 23% from 2019.

It's gotten so bad, Microsoft and Apple now warn people about various

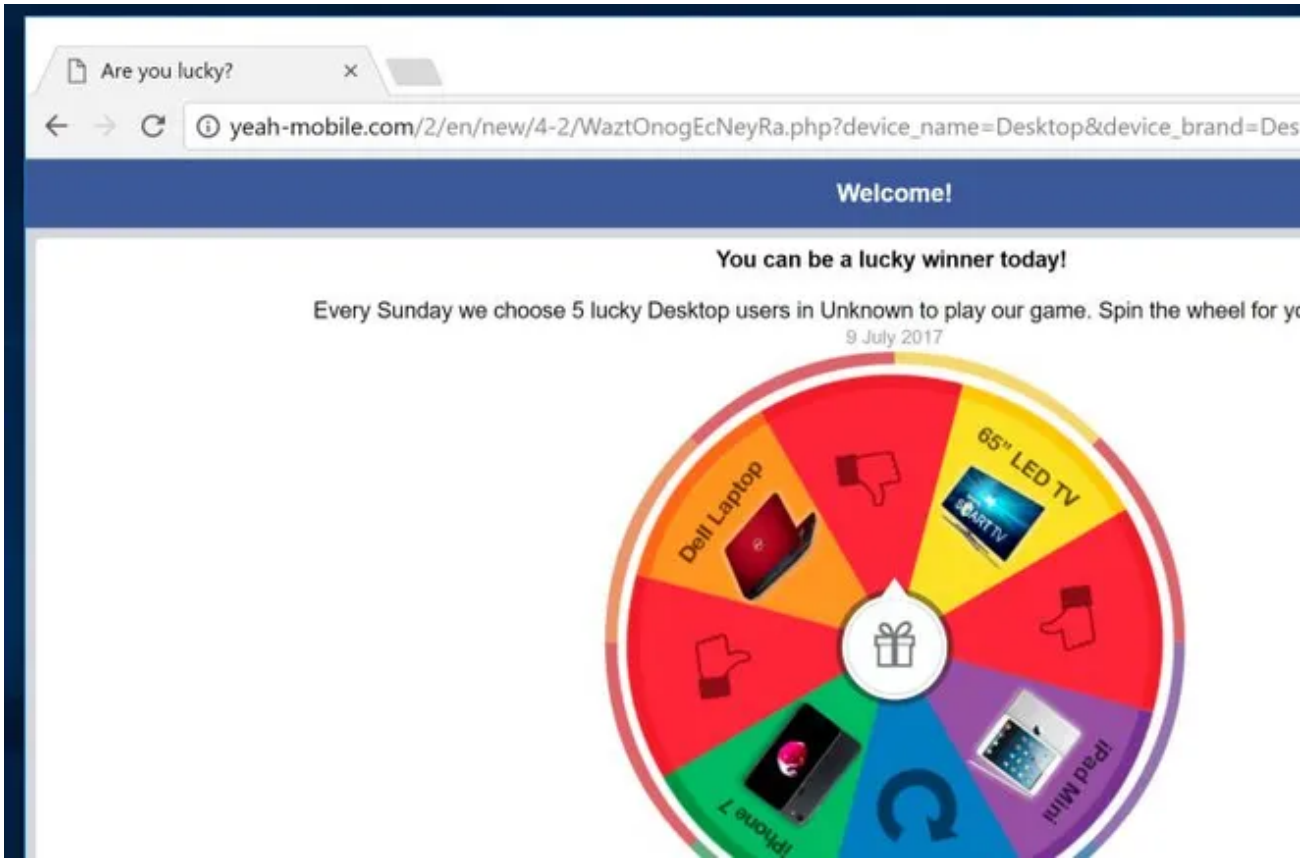
iterations of this scam on their websites. The FTC, FBI, and AARP are also trying to get the word out about it. But the cyber-swindler's tricks are evolving and becoming more convincing every day.

“If this is your first encounter with this type of sociopathology, the most dangerous thing you can do is think you’re too smart to fall for it,” warns Bob Sullivan, consumer security expert, and host of AARP’s Perfect Scam podcast. “They’re really good at these quick emotional flips and putting you in a panic state very quickly. That’s when you’re ripe for the taking.”

How it works

The scammers might call you directly on a landline or cell phone, or send a phony email, text message, calendar invite, or even direct message via social media. They may “spoof” the phone number so that it looks like a legitimate call from a trusted company, or from someone in your own area code.

In my moms' case, the crooks initiated contact by using a scam pop-up ad via her Chrome browser. It warned that her device was compromised, hackers were controlling it, and to call the number on the screen or risk losing everything on the laptop, including her identity, passwords, and even access to her bank accounts.



Fake pop-ups are fairly common — many of us have seen that scam "prize alert" message at least once in our connected lives. It most often happens if you click on a dodgy website by mistyping a URL or following a nefarious link from a spam message.

No matter how the thieves deliver the threat, the immediate result is often the same. "You panic, and want to fix it," Sullivan explains. "If you call the number you get a really nice voice on the other end, reiterating what grave danger you're in, but that they will, in essence, keep you from the real harm."

Once they get you on the phone, the real hustle begins. The scammer says he's a certified Apple (or Microsoft, or any other well-known company) technician, and offers to give you his certification number. The talk is fast, smooth, and the crook has an answer for everything.

“You asked a lot of good questions and at every turn, they were ready with what seemed like a sensible answer, Sullivan tells my mother directly over Zoom. “And that’s because they have practiced this, they’re running dozens of these every single day.”

The fake technician might ask you to download an app that allows them to “run a diagnostic test.” Then they pretend to spot all kinds of horrible hacks, and either offer to fix it, maybe for a price, or download more software — which likely infects your machine with malware for real.

“He told me to download TeamViewer from [Apple’s] App Store, and that it would let him see my desktop, but not take control of it,” my mother recalled. “Then he said ‘we’re going to do some testing on your bank accounts to make sure they’re secure. We’re going to transfer some money from your savings to your checking. When that worked, he said I should transfer money to the official technician account through Zelle, which I had never heard of. But he explained that it’s part of my bank, and fraud protected just like my bank accounts and credit cards, and not to worry because it would go out and come right back in. He also said all of this service was ‘free’ from Apple.”

This is the part of the story where I put my head down on my desk and groan out loud, “Mom, why did you think this was real? Why didn’t you call me?”

“I trust Apple. I trust my [USAA] bank, and because Zelle was right there on the USAA site, I trusted that too.” The scammer did take money out of her account and put it all (she thought) right back in. He then sent her off on a wild goose chase to buy Target gift cards for some other convoluted diagnostic test, and that’s when she finally called me — five hours after first responding to the alert on her laptop.

By then a blaring alarm was going off on her laptop and she didn't think she could turn it off. "Just shut the lid," I said. Of course, that made the horrible siren noise stop, but she's far from over the entire ordeal.

You have been scammed. Now what?

The first thing I had my mom do was contact USAA and report the fraud. Then, block the swindlers' phone number.

Scammers are relentless. They kept calling back after my mom hung up, so it's important to block the calls, and not answer any more from numbers she doesn't recognize. (If it's legitimate, people leave a message.)

I also had her change all of her passwords, report the scam to several authorities including the FTC and FBI, back up her files, and do a full reset and restore of her MacBook, iPhone, and iPad.

Some people suggest running additional anti-virus software too. "You can make an appointment at an Apple Store or contact Apple Support online, tell them what happened, and see if there are any additional precautions they suggest," Sullivan said.

The next day, while monitoring her bank accounts, she saw that three of the five Zelle money transfers were returned. But $2,000 is still missing.

USAA told her there is nothing they could do because she had authorized the transactions through Zelle. She contacted Zelle, and they too told her she won't get her money back.

"We caution consumers in all of our marketing and consumer

education," says Meghan Fintland, a spokesperson for Zelle we contacted for this story. "Zelle is only to be used to pay people you know and trust. Use it like you would cash because once you send the money, it is gone in minutes and you can't get it back."

"I am the head of Fraud and Central Operations for USAA Bank, and my parents have fallen victim," Stacey Nash, SVP, Bank Fraud Management, and Operations wrote to me via email. "Elder financial abuse is something we train to detect and do awareness campaigns to prevent. It can happen to anyone, but it's particularly disheartening when it's your elderly family member."

"It's my fault for being too trusting I guess," my mom says. "Maybe it's a generational thing. I don't know. I'm sure $2,000 doesn't seem like a lot of money to some people, but it's a lot for us. I just hope sharing this keeps someone else from getting scammed."

How to keep from getting scammed

Apple and Microsoft walk you through the do's and don'ts of this tech support scam and other popular frauds on their sites. AARP offers a class in spotting scams and has a whole webpage warning people of the dangers. The best advice includes:

Apple, Microsoft, and other reputable tech companies do not contact customers about "tech support," unless the customer initiates communication — period.
If a pop-up or error message appears with a phone number, don't call the number. Error and warning messages never include phone numbers.
If you get a tech support scam pop-up, close the browser. On a

Windows PC, press Control-Alt-Delete to bring up the Task Manager. On a Mac, click on the Apple icon in the upper left corner of your screen and use the Force Quit command.
Never pay for tech support or other services with a money-transfer app, gift card, cash-reload card, or wire transfer.
If you get a call, don't answer. If you answer, hang up, and block the call. Once scammers know they reached a working number, you become a recurring target. One of the most common scams after you engage with cyber-crooks over fraudulent service— is the "refund scam."
Never trust any company — tech or otherwise — requesting personal or financial information.
Keep your security software, browser, and operating system up to date, and consider using your browser's pop-up blocker.

Last, but not least, remember when we were taught to stop, drop, and roll, if our clothes catch on fire? Sullivan says it's a great rule of thumb to keep from getting burned by modern scams too. "Whenever you're in one of those moments where you think, 'Oh my God, something terrible might be happening,' stop what you're doing. Drop the mouse, and roll your chair away from the desk."

Then, call someone you trust. Like your daughter.

Jennifer Jolly is an Emmy Award-winning consumer tech columnist and host of USA TODAY's digital video show TECHNOW. Email her at jj@techish.com. Follow her on Twitter: @JenniferJolly.

The views and opinions expressed in this column are the author's and do not necessarily reflect those of USA TODAY.