# Social Engineering: Beware of ‘Tech Support’ Scams

Kirk McElhearn


It begins with a simple phone call. A scratchy voice, often sounding distant and foreign, introduces the caller as "John," or "Steven," but the accent suggests otherwise. The caller claims to be calling from Microsoft tech support, and says that there's a problem with your computer. If you say that you have a Mac, they either hang up or say, "Yes, sorry, you have a Mac."

And so begins an attempt at *social engineering* (social hacking), a way of conning people into allowing an unknown person to access their computer, possibly copy files, and eventually getting them to pay for this "tech support." The scammer strings the user along, leads them to supposed "error" messages and malware files on their computer, and gets them to install software

allowing the scammer to access their files.

Even though Microsoft recently stated that only 183,000 had reported this type of scam to the company in 2017, that's probably just a fraction of the number of people who get contacted; it's a very common scam. Most tech-savvy people know that this is a scam and just hang up, but as with phishing scams, it only takes a few people to be tricked to make the scam worthwhile.

## Social engineering is big business

Tech support scams are a kind of social engineering, a technique that conmen use to persuade people to give them money, or more, for illegitimate reasons. When well executed, scammers can be quite convincing, but these tech support scams tend to be carried out by people in poor countries with limited English skills, making them easy to detect.

Social engineering is used to glean information from users—bank details, credit card numbers, Microsoft logins or Apple IDs. The goal is often to install malware on a user's computer, so they can access it remotely, copy its files, or even lock down a user's documents as part of a ransomware attack.

One security researcher got contacted by a tech support scammer and played along to investigate how the process worked. He did this, he said, because "Many of my family members have received these calls, so I wanted to play the game to see how the scam worked." His video shows how this process happens, and the types of tricks the scammers use.

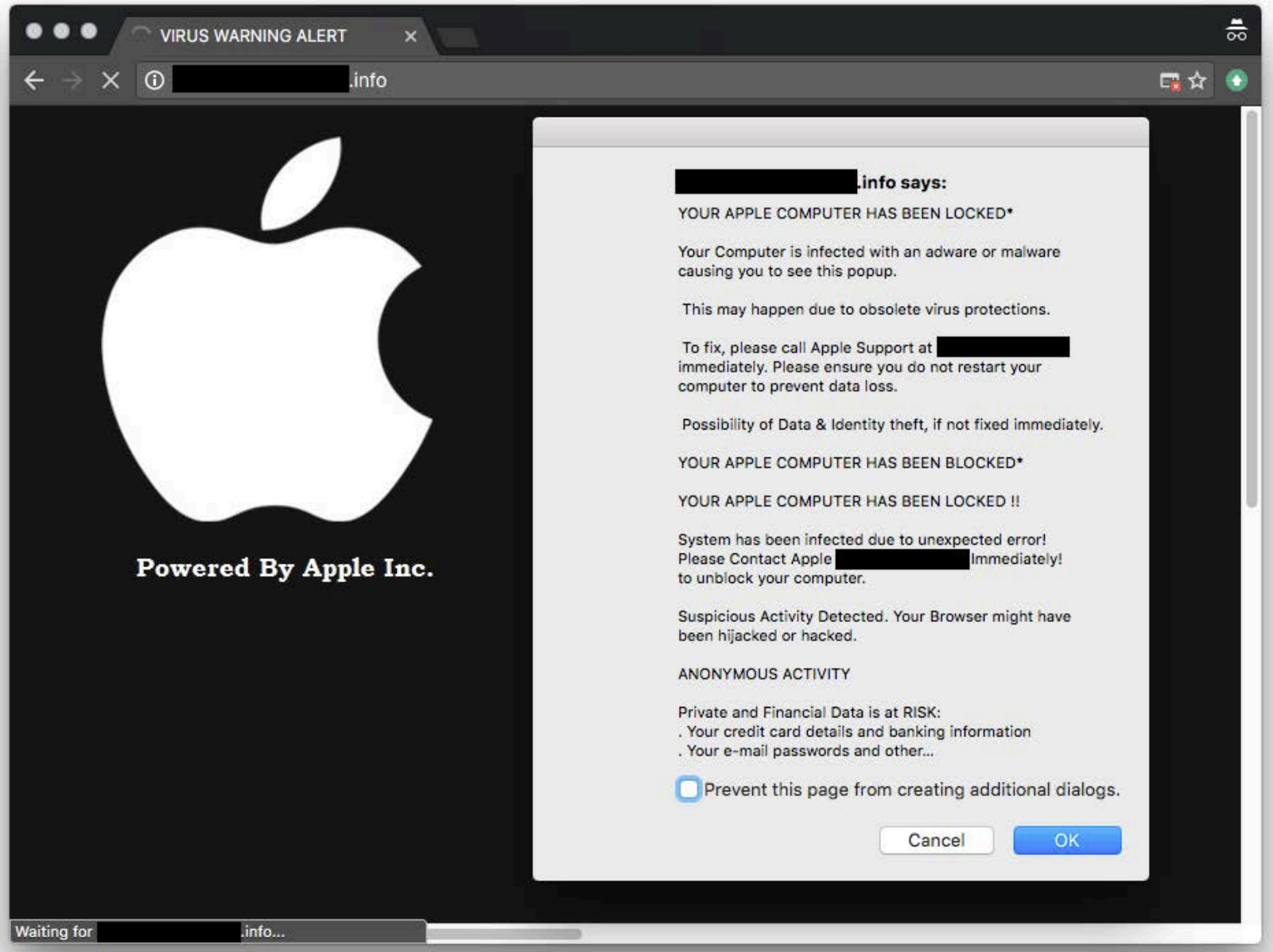
They start by hooking the victim, and then convincing them that there is an issue. They persuade the user to install remote administration software, so they can take control of the computer. They show the user "threats," which are merely files that users never see. They explain that they can solve the problems for a (not so small) fee. And then they cash in.


Tech Support Scam Process (Image credit: Microsoft)

The truth is no one will ever call you out of the blue to tell you that you need tech support on your computer. In some cases, these are just random cold calls hoping to find someone who has a computer; fewer people use desktop computers at home these days, making the targets less common. In other cases, scammers may target people who have shared information about a new computer on Facebook, Twitter, or other social media platforms.

## Tech support scams on the Web

These scams don't only occur through phone calls—they also flourish on the Web. You may visit a website and see a dialog suggesting that your computer is infected with malware, and giving you a phone number to contact to get help. Often, these dialogs use the Windows XP interface, but sometimes you see Mac dialogs, like this one:




It's probably obvious that this is bogus, but the reality is there are plenty of people who fall for these scams. And some of these dialogs look more convincing, but no dialog on a Mac or PC will ever give you a phone number to call to resolve a problem. As with the cold calls, they hope to snag a small percentage of people, because they cast their nets very wide, displaying their messages to millions. If one tenth of one percent of people fall for the scam, that's potentially a lot of money.

If you're reading this, you probably already know about these social engineering scams. What's important is that you tell others—your friends and family, especially older, less tech-savvy people—about this, so they know that when the scammer calls, they should just hang up.

***Have you ever been called by a tech support scammer? Ever***

***fallen victim to a social engineering attack? We want to hear you story! Drop us a comment below.***

## About Kirk McElhearn

**Kirk McElhearn** writes about Macs, iPods, iTunes, books, music and more on his blog Kirkville. He is co-host of The Committed: A Weekly Tech Podcast, and a regular contributor to The Mac Security Blog, TidBITS, and several other websites and publications. Kirk has written more than twenty books, including Take Control books about iTunes, LaunchBar, and Scrivener. Follow him on Twitter at @mcelhearn. View all posts by Kirk McElhearn →