Lockdown: Apple could make it even tougher to hack Phones

February 24 2016, by Michael Liedtke

Protesters carry placards outside an Apple store Tuesday, Feb. 23, 2016, in Boston. Demonstrators are expected to gather in a number of cities Tuesday to protest the FBI obtaining a court order that requires Apple to make it easier to unlock an encrypted iPhone used by a gunman in December's shooting in San Bernardino, Calif. (AP Photo/Steven Senne)

Suppose the FBI wins its court battle and forces Apple to help unlock an iPhone used by one of the San Bernardino killers. That could open all

iPhones up to potential government scrutiny—but it's not the end of the story.

Turns out there's a fair bit both individuals and Apple could do to FBI-proof their phones and shield private information from investigators and cybercriminals alike. Those measures include multiple passcodes and longer, more complex ones.

Of course, increased security typically comes at the expense of convenience. Most efforts to improve phone security would make the devices harder to use, perhaps by requiring you to remember more passwords.

Making it more difficult for law enforcement to crack open iPhones could also spur legal restrictions on phone security, something that neither Apple nor other technology companies want to see.

"They are walking a tightrope," says Mark Bartholomew, a law professor at the State University of New York at Buffalo who specializes in privacy and encryption issues. Requiring longer passcodes might annoy most Apple users, he says, while boosting phone security "sort of amplifies the whole argument that Apple is making things too difficult and frustrating law enforcement officials."

A New York police officer stands outside the Apple Store on Fifth Avenue while monitoring a demonstration, Tuesday, Feb. 23, 2016, in New York. Protesters assembled in more than 30 cities around the world to lash out at the FBI for obtaining a court order that requires Apple to make it easier to unlock an encrypted iPhone used by a gunman in December's mass murders in California. (AP Photo/Julie Jacobson)

Apple had no comment on any future security measures. In a recent letter to customers, it noted that it has routinely built "progressively stronger protections" into its products because "cyberattacks have only

become more frequent and more sophisticated."

In the current fight, the FBI aims to make Apple help it guess the passcode on the work phone used by Syed Farook before he and his wife killed 14 people at an office party in December. The FBI wants Apple to create special software to disable security features that, among other things, render the iPhone unreadable after 10 incorrect guesses.

Apple has resisted, maintaining that software that opens a single iPhone could be exploited to hack into millions of other devices. The government insists that its precautions would prevent that, though security experts are doubtful.

Should the FBI prevail, it would take computers less than a day to guess a six-digit passcode consisting solely of numbers, the default type of passcode in the latest version of the iPhone operating system. Even with security features disabled, each passcode guess takes 80 milliseconds to process, limiting the FBI to 12.5 guesses per second.

For security-conscious individuals, the simplest protective move would be to use a passcode consisting of letters and numbers. Doing so would vastly increase the amount of time required to guess even short passcodes. Apple estimates it would take more than five years to try all combinations of a six-character passcode with numbers and lowercase letters. Adding capital letters to the mix would extend that further.

A pedestrian walks by the Apple Store on Fifth Avenue while avoiding a small demonstration held along the sidewalk, Tuesday, Feb. 23, 2016, in New York. Protesters assembled in more than 30 cities around the world to lash out at the FBI for obtaining a court order that requires Apple to make it easier to unlock an encrypted iPhone used by a gunman in December's mass murders in California. (AP Photo/Julie Jacobson)

Changing to an alphanumeric code is as simple as going into the phone settings and choosing "Touch ID & Passcode," then "Passcode options."

Another option is simply to pick a much longer numeric code. An 11-character code consisting of randomly selected numbers—that means no references to birthdays or anniversaries that could be easily guessed—could take as long as 253 years to unlock.

But longer, more complex codes are harder to remember, and that's probably why Apple hasn't yet required their use. It could, however,

easily do so. In fact, iPhones moved to six-digit passcodes from four last September.

Apple may have other tricks up its sleeve. For instance, the company could add additional layers of authentication that would thwart the security-bypassing software the FBI wants it to make, says computer security expert Jonathan Zdziarski.

Apple phones rely on a feature known as the "secure enclave" to manage all passcode operations. The software demanded by the FBI would alter the secure enclave, Zdziarski says. But the software couldn't do so if the secure enclave required the user passcode to approve any such changes.

"This is probably the best way to lock down a device," Zdziarski says.

Apple could also require a second passcode whenever the phone boots up; without it, the phone wouldn't run any software, including the tool the FBI is requesting. "It would be like putting a steel door on the phone," Zdziarski says. Currently, iPhones automatically load the operating system before asking for a passcode.

For now, Apple CEO Tim Cook is focusing on winning the current battle with the FBI in a Southern California federal court while also trying to sway public opinion in the company's favor. The skirmish could go all the way to the U.S. Supreme Court.

In the meantime, Apple is probably already working on security improvements for the next version of the iPhone operating system that it will probably announce in June and release in September.

Citation: Lockdown: Apple could make it even tougher to hack Phones (2016, February 24)