Has Apple done enough to fix celebrity photo leaks?

John
Brandon

Apple CEO Tim Cook, holding an iPhone 6 Plus, discusses the new Apple Watch and iPhone 6s on Tuesday, Sept. 9, 2014. (AP Photo/Marcio Jose Sanchez)

There's nothing like a big distraction to divert attention. After Apple unveiled the iPhone 6 and the Apple Watch on Tuesday, questions lingered about one of the most high-profile security leaks of the last decade: the theft of 101 nude photos of well-known celebrities from Apple's iCloud service on Aug. 31.

In an interview with the Wall Street Journal last week, Apple CEO Tim Cook blamed the attack on phishing scams whereby hackers get hold of passwords, as opposed to weaknesses in the tech giant's security. Nonetheless, Apple has promised tighter security features following the celebrity photo hack.

During Tuesday's keynote address and product demos, however, the only "leaks" that were mentioned were a nod to how attendees already knew about the bigger iPhone models. Security came up only when the company announced plans to offer a mobile payment service called Apple Pay.

"It's the typical Apple culture of denial," says security expert Winn Schwartau, author of the book 'Information Warfare.' "They never admit mistakes," he added.

For the past year, Apple has offered optional 'two-step,' also known as 'two-factor,' authentication for the Apple ID you enter to make purchases on iTunes. The feature sends a one-time code to your smartphone after you type in your password. To gain access, you have to type in the code.

The company says it will roll the feature out to iCloud in the coming weeks. Also, users will be notified if someone tries to log in to their iCloud account from an unrecognized device.

Many other tech giants, including Google, Twitter and Facebook, already offer two-step authentication.

By offering this new security measure, Schwartau says, Apple is essentially admitting that a brute force attack helped hackers gain access to celebrities' passwords, and that they likely used a password generator. By adding the new authentication, he says, Apple is making it harder to do a brute force attack.

Tasso Roumeliotis, CEO and founder of the secure mobile app firm Location Labs, says Apple is shirking its responsibility by blaming iCloud users – the celebrities who used the service – for not using strong passwords.

Apple reps have said in public statements that it's a common problem on the Internet for people to use weak passwords and for hackers to steal data after guessing the password. (The company declined to comment on the record when asked about offering additional security practices.)

Some reports have suggested the hackers used a phishing scam by sending fake text messages to celebrities and asking for a password reset. Schwartau says this would assume the hackers had access to their phone numbers. Others have suggested the hackers snooped on an open Wi-Fi network, but Schwartau says that's also unlikely because even open networks have some form of security in the browser or app.

"I believe Apple could have offered stronger language to keep their consumers confident that their platform is strong, and that hackers were successful because of weak passwords rather than software vulnerabilities," said Carlos Montero-Luque, the CTO at Apperian, a cloud computing company. He added that even two-step authentication won't help if hackers break into the back-end server that holds the information, which was unlikely in this case, he says.

"While the emphasis is being placed on enabling two-step authentication, reports suggest that this currently does not protect iCloud backups, meaning a determined attacker could restore from a previous iCloud backup without the second [authentication] step," says Satnam Narang, a security response manager at the security company Symantec.

Roman Foeckl, CEO and founder of the security firm CoSoSys, said the "missing ingredient" in Apple's response is communication. He said customers need to know more about how to protect their data on an iPhone, on a Mac and in the cloud. He said Apple has the opportunity to use its greatest assets – engineering prowess and the ability to make technology easy to use – to strengthen its security.

"Apple could be an industry leader in security and privacy," added Roumeliotis. "Think about the forgotten password flow [what users have to do when they forget a password, such as answering a security question]. Apple has so many chances – from customers' biometric information to their linked devices – to send customers clear, easily understood messages about what the secure experience is, then deliver it. As of today, they don't."

At the very least, the leaked photos should be a wake-up call. Tech companies will share some of the responsibility for user security, but not all of it.