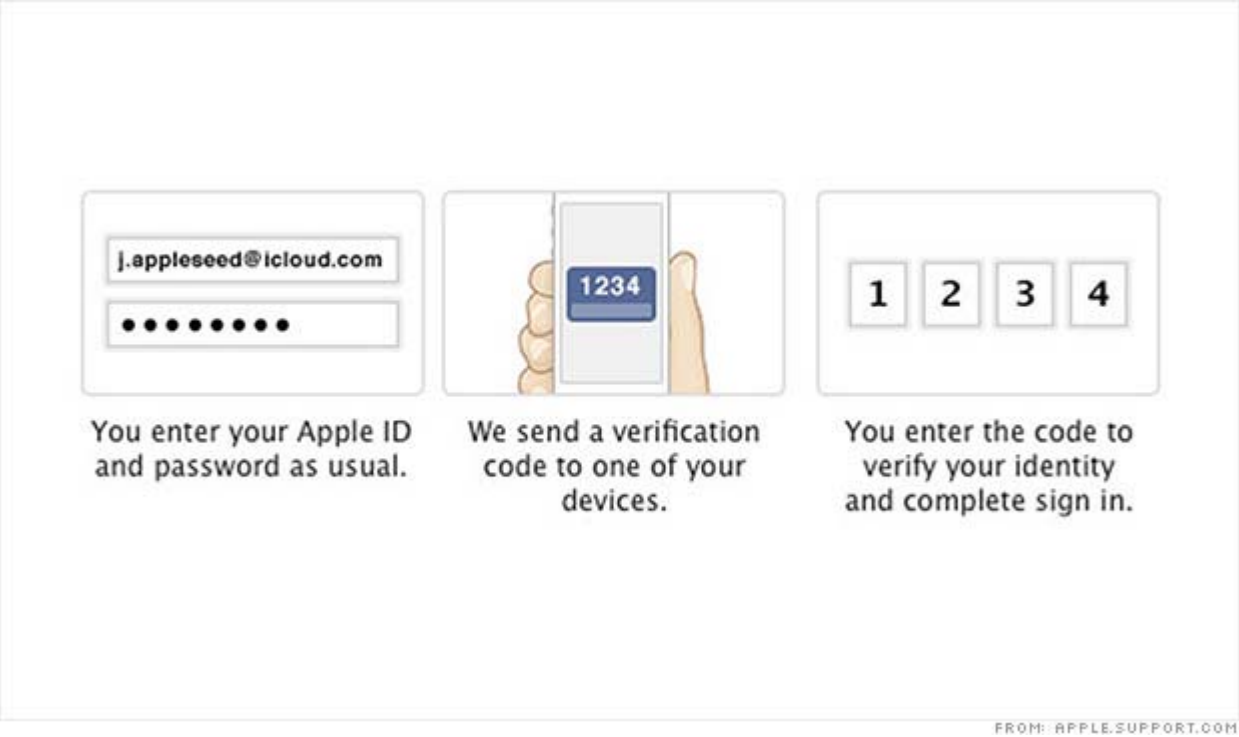
Apple's new security system has holes

By Julianne Pepitone @julpepitone May 30, 2013: 6:08 AM ET

http://cnnfn.cnn.com/2013/05/30/technology/security/apple-security/index.html?iid=HP_LN



Apple added a two-factor authentication option for Apple ID, but security holes in the system leave personal information at risk.

NEW YORK (CNNMoney)

Apple recently beefed up its authentication system in an effort to thwart hackers, but a new report shows the security measure is lacking in one huge area.

Back in March, Apple (AAPL, Fortune 500) unveiled an optional "two-factor authentication" login method for its Apple ID. It's a basic security tool already used by Google (GOOG, Fortune 500), Facebook (FB) and Dropbox that requires both a password and a piece of data, such as a string of numbers sent via text message. Twitter also recently unveiled such a system following a series of prominent hacks of Twitter accounts.

But security software company ElcomSoft explained in a blog post Thursday that Apple's new security measures protect users only in a few situations: app and music purchases, managing an Apple ID account or receiving customer support related to Apple ID. It does nothing to protect other important information, like photos and other files stored on its iCloud service.

A hacker who manages to figure out a user's Apple ID and password could log into that user's iCloud account, and download all of the potentially sensitive information stored there -- even if that user has the two-factor system enabled. ElcomSoft accused Apple of doing "a half-hearted job," arguing the two-factor protection should be implemented on iCloud data backups as well.

ElcomSoft laid out how a hacker could download that data by using a compromised Apple ID account to log in and restore a device's settings through an iCloud backup. Or the attacker could also use a simple program to download a user's iCloud data onto a computer.

Apple does send an email alerting users when a new device is restored using an iCloud backup, but ElcomSoft didn't receive a message after using a program to download the data.

"Apple's approach in implementing two-factor authorization does not look like a finished product," ElcomSoft wrote in its blog post. "It's just not as secure as one would expect this solution to be."

An Apple spokeswoman declined to comment, and ElcomSoft said it got the same response.

To be fair to Apple, the company never said its two-factor system would protect iCloud. ElcomSoft wrote in its blog post that the system "does everything that it claims to be doing." But as the software company points out, Apple's system simply isn't as robust as it could be. And users may assume that implementing two-factor authentication has them covered across the board.

"As usual, Apple refuses to comment on anything concerning security, so we can only guess whether or not the two-step protection will be extended to cover information stored in the iCloud," ElcomSoft wrote in its post.

While the iCloud problem was by far the biggest issue ElcomSoft raised, the company also listed other concerns.

For example, when a user enables two-factor authentication, the verification code is sent as a "FindMyPhone" message -- that is, a message that appears on the screen of a device even when it's locked. That's almost certainly because iPods and iPads can't receive text messages. But it is a problem if an Apple device is lost or stolen and anyone can easily see the verification code.