Celebrity hack puts focus on Internet 'cloud' (Update)

September 2 2014, by Rob Lever

If actress Jennifer Lawrence and model Kate Upton knew little about the Internet "cloud," they would not be alone, but the recent theft of their intimate photos has served as a wake-up call.

Hackers have boasted of stealing nude pictures of dozens of celebrities—including singer Avril Lavigne, actress Hayden Panettiere and United States soccer star Hope Solo.

And, while some of the pictures appear to have been faked, several A-listers denounced an invasion of their privacy after pictures popped up on anonymous online bulletin boards.

What is the Internet cloud?

The cloud refers to storage of data on large-scale shared servers rather than on users' own home hardware.

It allows people to access their documents and pictures remotely on multiple devices such as PCs, smartphones and tablets from anywhere with an Internet connection.

Hackers appeared to access photos stored in Apple's service called iCloud, which backs up photos and other documents from iPhones. As a result, the private pictures of the female celebrities became public and spread across social media, starting with the image-sharing service

4chan.

Apple, in its first public statement on the incident, said celebrity accounts were compromised in a "targeted attack" to gain passwords, but maintained that it found no breach of the iCloud or other Apple systems.

What is in the cloud?

People can choose to back up pictures, videos and other files in the cloud. In some cases smartphones and other devices will do this by default—a fact not all users are aware of.

"Many iPhone owners are possibly oblivious to the fact that every time they take a photo, it is invisibly and silently uploaded to iCloud in the background," says computer security consultant Graham Cluley in a blog post.

The private pictures of Lawrence, Upton and others appeared to have been stored in these cloud servers, even if they were deleted from the phones or other devices used to take the pictures.

Is the cloud secure?

Major services like Apple's iCloud and Google Drive use encryption to secure data. But Rob VandenBrink at the SANS Internet Storm Center said a flaw in Apple's "Find My iPhone" app lacked protection against "brute force attacks" from hackers.

"And of course once an account password is successfully guessed, all iCloud data for that account is available to the attackers," VandenBrink said in a blog post.

"So no rocket science, no uber hacking skills. Just one exposed attack surface, basic coding skills and some persistence."

Are passwords involved?

Because many people use easy-to-guess passwords like "123456" and reuse them across multiple services, hackers often can gain access with little difficulty.

Rik Ferguson at the security firm Trend Micro said attackers could have used the "I forgot my password" link for Apple accounts.

"The peril in this for celebrities is that much of their personal information is already online and a security question such as 'Name of my first pet' may be a lot less secret for a celebrity that it is for you and I," Ferguson says.

A better system is to activate two-factor authentication, which sends an additional code to a predetermined email or phone.

Are there other vulnerabilities?

An old technique used by hackers known as "phishing" can get a user to hand over a password voluntarily. This often begins with an email which says an account has been compromised and requests that the user log in via a link.

Symantec security response manager Satnam Narang said his firm has been warning about fake emails or SMS messages claiming to come from Apple technical support.

The comedian Sarah Silverman tweeted recently: "I got a text from apple

privacy security saying my iTunes id has been compromised—HOW DO I KNOW THEYRE NOT THE SCAM? Help!"

Narang said these kinds of hacks are likely to continue because many people fall for the scams.

"Users should also be wary of emails or text messages claiming to be from Apple support, security or protection groups. Don't click on any links in these emails and never send your Apple ID credentials in a text message," he said.

Chris Morales at NSS Labs said Apple "is doing what everyone else in the industry is doing" to make its system easy to use, which also makes it easier to hack.

"The cloud is so convenient, so everybody is putting their whole lives in the cloud," he said.

© 2014 AFP