'Cloud' focus after internet hack

WASHINGTON, USA: If celebrities like actor 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 for everyone.

Security expert Graham Cluley says most people are unaware that iPhones automatically back-up their information to the iCloud service where it is accessible to anyone with the right passwords. Image: Graham Cluley

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.

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.

People can choose to backup 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.

Default setting on iPhones upload to iCloud

"Many folks are blissfully unaware about iPhone photos being automatically sent to an Apple iCloud internet server after it is taken," says Computer Security Consultant Graham Cluley.

"That's great in some ways - it means it's easily accessible on other Apple devices - but might be bad in others."

Major services like Apple's iCloud and Google Drive use encryption to secure data. But Rob VandenBrink at the SANS Internet Storm Centre 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 huge hacking skills. Just one exposed attack surface, basic coding skills and some persistence is all that's needed," he said.

Trend Micro's Rik Ferguson says the "I forgot my password" message can be used by hackers to access other people's accounts. Image: ITP

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.

Easy to guess passwords

"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.

Symantec's Satnam Narang warns that fake emails and SMSs are being used to solicit passwords from users. Image: Twitter

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

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 THEY'RE NOT THE SCAM? Help!"

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

"Because of the continued narrative surrounding iCloud as the point of compromise, we expect to see more successful phishing attempts of Apple IDs," he said in a blog posting.

"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 warned.

Source: AFP via I-Net Bridge