



## 5 things to note about iCloud security

*Ellyne Phneah, ZDNet Asia on November 1st, 2011 (3 hours ago)*

**Apple's new iCloud service is touted to allow consumers to store their data on Cupertino's servers and access and transfer the data between devices and applications. However, like any cloud application, iCloud users will face potential risks when it comes to data security and privacy.**

While [iCloud](#) makes it "extremely easy" for users to keep and sync large amounts of personal data in the cloud, it can also expose data to numerous security risks including virus infections and wireless vulnerabilities, warned CoSoSys' founder and CEO, Roman Foeckl. It can also lead to hacking attempts resulting in data theft, the Romania-based analyst told ZDNet Asia.

"This is an example of emerging technology that focuses on making everything easy to use, readily available and highly mobile," Foeckl said. "It should in no way be avoided, but just to be used cautiously in order to avoid the associated risks."

ZDNet Asia spoke to security players and identified five security issues users should bear in mind with the iCloud service:

### **1. No visibility on data.**

Scott Chasin, CTO of McAfee's content and cloud security, pointed to an overriding concern over the lack of transparency as users have no visibility on what happens to their data.

Elaborating, he explained that when using Apple products, users still do not have clear answers to fundamental questions about transparency such as "Is it protected and encrypted?" or "How is it being backed up?"

"While the tagline for iCloud simply states, 'It just works', consumers and businesses alike need to remember that Apple has yet to publicly address security around iCloud, as it has with previous releases of the iOS platforms," Chasin warned. "[Users] may have to think twice before trusting iCloud with important data."

### **2. One password to rule them all.**

Macky Cruz, technical communications specialist at Trend Micro's TrendLabs, also noted that the iCloud account is governed by a single user ID, which may make it more difficult for consumers to safeguard themselves and their information.

"The only protection is the Apple ID and its password," David Jacoby, senior security researcher of Nordics global research and analysis team at Kaspersky Labs, said in an e-mail interview. "If you can obtain that, you can import e-mail, pictures, calendar and possibly even more."

The Sweden-based analyst recommended that Apple users [adopt strong passwords](#) which is not easily deduced. Jacoby added that they should also make sure they do not connect to wireless networks [that they do not trust](#) as an attacker in the network could potentially obtain their passwords and sync their Apple accounts to his own computer.

### **3. Data syncing convenient but insecure.**

One of the benefits touted by iCloud is that consumers can sync across their Apple devices with a single

data set, but this also means that the data can be manipulated from a single device should it be lost or stolen, Chasin remarked.

"The most important thing for users is to ensure they are aware that their data is being synced to iCloud," he said. "Where necessary, users can simply turn off iCloud syncing for documents, data backup and photos if they choose to."

#### **4. Allowing iCloud to access, store corporate information.**

From the enterprise perspective, companies that allow their employees to [access corporate data](#) via their personal Apple devices must decide if they are comfortable to extend this to the iCloud, noted Trend Micro's Cruz, adding that this is an [issue for any cloud](#) implementation.

Chasin noted that concerns about allowing the Apple cloud service to store and access corporate data can also arise in situations where employees, who own personal Apple devices containing business information, lose their devices in a taxi or leave the company.

Cruz said: "There are reasons to be concerned about iCloud. Many employees have started [using personal devices for work purposes](#) and companies must decide if they are comfortable with their intellectual property being linked to the cloud."

#### **5. User privacy at risk.**

Like any other cloud providers, data stored via iCloud must be revealed when a subpoena is issued to Apple, Chasin warned, and users syncing their data to Cupertino's cloud service should be aware their data could be revealed to authorities under these circumstances.

Because iCloud stores and replicates all data across individual Apple devices, there can be a breach of privacy should any of the device be misplaced, Cruz added.

Confidential data such as health records which Apple users intend to backup in the cloud service need to be encrypted when stored on their devices, advised Foeckl of CoSoSys. "This way, when transferred into the iCloud, it will still be encrypted so even when it is accessed or stolen, it cannot be easily used," he said.

**URL:**<http://www.zdnetasia.com/5-things-to-note-about-icloud-security-62302711.htm>