How to protect your cloud data from hacks

By **John D. Sutter**, CNN
August 9, 2012 -- Updated 1442 GMT (2242 HKT) | Filed under: **Web**

Cloud data storage is becoming more popular, but it's not without risk.

STORY HIGHLIGHTS

- Security experts offer tips on how to use the cloud safely
- Back up your files in multiple places, including in on-the-ground hard drives
- Use a different password for every website and social network
- Turn on Google's and Facebook's two-factor authentication features

(CNN) -- The cloud sounds amazing.

Set up your entire digital life to sync automatically with a server run by some big (ostensibly responsible) tech company, and you never have to worry about losing data again, right?

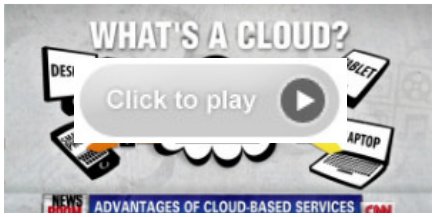
Wrong, of course. As a Wired writer's recent brush with hackers shows, there are plenty of ways for your cloud-based accounts -- Amazon, Apple, Google -- to be hacked. And while both Amazon and Apple responded to Mat Honan's story (you should read the whole thing; he says he lost all his pictures of his young daughter in the attack) by at least temporarily changing their policies in hopes of better protecting consumers, there are still plenty of cloud-related precautions security experts say you should take.

These go beyond just setting passwords that aren't "12345." (Hopefully you made that switch in 1998. Hopefully.)

Here are five of the best cloud-safety tips we could rustle up:

1. Backup everything -- in the cloud and on the ground.

In his account for Wired, Honan writes that he doesn't actually blame the person who hacked him for the fact that he lost all of the data on his laptop. "I'm mostly mad at myself," he writes. "I'm mad as hell for not backing up my data. I'm sad, and shocked, and feel that I am ultimately to blame for that loss."



What is cloud computing?

Robert Siciliano, an online security expert at McAfee, said people should back up their data not only with a cloud service such as iCloud, Mozy or others but also on "at least two, three or four" real-life hard drives. For maximum protection, put these backups in multiple locations.

"You don't want to have all your eggs in one basket," he said.

2. Use a bunch (maybe hundreds?) of different passwords.

Here's another one from Siciliano: Create different passwords for every single online account.

"I have 700 and something passwords," he said.

You can use a password management service such as RoboForm or LastPass to generate hard-to-guess passwords and to store them on the devices you use most often. Other security experts recommend writing the passwords down in one place and storing that paper in your wallet -- although that could pose a security risk if your wallet is stolen.

3. Don't link all of your accounts together.

This is sometimes called daisy-chaining, and Honan writes that it's one of the things that did him in. If you use Facebook, Twitter or Google to log in to other social networks or websites, you may run the risk of all those accounts being compromised at once. Siciliano said it's OK to link accounts sometimes, but you should try to think like a hacker when you're doing it.

"Connect accounts," he said, "but you have to reverse engineer the process. What could a bad guy do if he got access to this account?" If he or she could get bank account info, reconsider.

4. Use two-factor authentication on Google and Facebook.

This one is key. Both Facebook and Google offer what's called "two-factor authentication" or sign-in. Google's Matt Cutts explained this in detail in a recent blog post called "Please turn on two-factor authentication." He writes: "Two-factor authentication means 'something you know' (like a password) and 'something you have,' which can be an object like a phone."

For example, Google will send you a code via text or voice message when you sign in. You'll then need your password and the code to log into your Google account from an unfamiliar computer if you have two-factor authentication turned on. "You can tell Google to trust your (other) computer for 30 days and sometimes even longer," Cutts writes.

Facebook, meanwhile, has a similar feature that it calls "Login Approvals." It's used when you log in from an unfamiliar computer. You have to turn both these features on. And, according to Wired's Kim Zetter, some other services, including Amazon, Rackspace and WordPress (with a plug-in) have two-factor authentication, using some of Google's tools.

Not every online service has these options. But "when a site has given you additional security options (like Gmail's two factor authentication which sends you an SMS when you try to log into your account) -- USE THEM!" Graham Cluley, a senior technology consultant at Sophos, wrote in an e-mail.

5. Don't use 'Find My Mac' on Apple computers.

Here's another one from Honan. If you use "Find My Mac," which is designed to help you locate your laptop in the event of a theft, you run the risk that a thief or hacker could wipe it clean, which is what appears to have happened to him.

"When you perform a remote hard drive wipe on Find my Mac, the system asks you to create a four-digit PIN so that the process can be reversed. But here's the thing: If someone else performs that wipe -- someone who gained access to your iCloud account through malicious means -- there's no way for you to enter that PIN," he writes.

Do you have tips of your own? Let us know in the comments.