Should you store your data in the cloud?

April 15, 2016 | BY Wendy Zamora

It's pretty simple to understand where a file goes when you save it on your PC. It lives on your hard drive, possibly housed in a set of folders you've created and organized yourself. That file is only stored on your computer, unless you decide to email it to yourself or save it on an external hard drive or USB.

Now what about the cloud?

At its most basic level, "the cloud" is just fancy-talk for a network of connected servers (a server is simply a computer that provides data or services to other computers). When you save files to the cloud, they can be accessed from a computer connected to that cloud's network. Now take that idea and multiply it to understand how the cloud works for you. The cloud is not just a few servers, but a network of many servers typically stored in a spaceship-sized warehouse—or several hundred spaceship-sized warehouses. These warehouses are guarded and managed by companies such as Google (Google Docs), Apple (iCloud), or Dropbox.

So it's not just some nebulous concept. It's physical, tangible, real.

When you save files to the cloud, you can access them on any computer, provided it's connected to the Internet and you're signed into your cloud services platform. Take Google Drive. If you use Gmail, you can access Drive anywhere you can access your email. Sign in for one service and find your entire library of documents and photos on another.

Why are people concerned with cloud security?

It's physically out of your hands. You aren't saving to a hard drive at your house. You are sending your data to another company, which could be saving your data thousands of miles away, so keeping that information safe is now dependent on them. "Whether data is being sent automatically (think apps that sync to the cloud) or driven by users uploading photos to social media, the end result is that it's all there somewhere being logged and stored," says Jérôme Segura, Senior Security Researcher at Malwarebytes.

And that somewhere is a place that's not in your direct control.

Risks of cloud storage

Cloud security is tight, but it's not infallible. Cybercriminals can get into those files, whether by guessing security questions or bypassing passwords. That's what happened in The Great iCloud Hack of 2014, where nude pictures of celebrities were accessed and published online.

But the bigger risk with cloud storage is privacy. Even if data isn't stolen or published, it can still be viewed. Governments can legally request information stored in the cloud, and it's up to the cloud services provider to deny access. Tens of thousands of requests for user data are sent to Google, Microsoft, and other businesses each year by government agencies. A large percentage of the time, these companies hand over at least some kind of data, even if it's not the content in full.

"Some people argue that they have nothing to hide, that they're not doing anything wrong, and couldn't care less if their private information is accessed, especially if it helps in the effort to track down terrorists," says Segura. "While there is no doubt that ready access to data is an invaluable asset for intelligence agencies, it is really important to remember that each individual has a fundamental right to privacy."

Benefits of cloud storage

On the flip side, the data you save to the cloud is far more secure than it is on your own hard drive. Cloud servers are housed in warehouses offsite and away from most employees, and they are heavily guarded. In addition, the data in those servers is encrypted, which makes hacking it a laborious, if not formidable, task for criminals. Whereas a malware infection on your home computer could expose all of your personal data to cybercrooks, and even leave your files vulnerable to ransomware threats. In fact, we recommend backing up your files to a cloud service as a hedge against ransomware.

Another benefit to storing data on the cloud is cost effectiveness and ease-of-access. You can store tons of data, often for free, using the cloud. Measure that against the number of external hard drives and USBs you'd have to purchase, and the difficulty accessing data once you've stored to multiple other devices, and you can see why cloud storage has become a popular option for businesses and consumers alike.

Final verdict

Yes, your data is relatively safe in the cloud—likely much more so than on your own hard drive. In addition, files are easy to access and maintain. However, cloud services ultimately put your data in the hands of other people. If you're not particularly concerned about privacy, then no big whoop. But if you have sensitive data you'd like keep from prying eyes…probably best to store in a hard drive that remains disconnected from your home computer.

If you're ready to store data on the cloud, we suggest you use a cloud service with multi-factor authentication and encryption. In addition, follow these best practices to help keep your data on the cloud secure:

- **Use hardcore passwords:** Long and randomized passwords should be used for data stored on the cloud. Don't use the same password twice.
- **Back up files in different cloud accounts:** Don't put all your important data in one place.
- **Practice smart browsing:** If you're accessing the cloud on a public computer, remember to log out and never save password info.