Where to store electronic information / files

Do I need to back up files that are already in cloud storage?

By: Linda C. Brinson

The cloud seems like the next big thing in data storage, but is it really foolproof?
RYASICK/GETTY IMAGES

More and more, individuals and businesses are turning to the cloud for data storage. For some, the primary reason is that the cloud is the easiest, surest way to back up photos, e-mails and all sorts of documents. Others choose the cloud because of space – the cloud makes a great storage option if the sheer volume of data on your computer threatens to overwhelm it.

But for many computer users, there is a nagging doubt: Are my files really safe in the cloud, or do I need to back up the backup? The debate has gotten more intense as cloud data storage has become widespread – despite some headline-making failures.

The whole phenomenon of cloud computing is evolving. Debates also rage about ownership of and access to data in the cloud. The answer largely depends on individual circumstances: How good is the cloud storage service you're using? And how vital is the data you're storing?

For most data that's of relatively minor importance, cloud storage is probably OK. For essential data, you might want to think seriously about the need for backup.

Coming up with a good answer means understanding what's involved. Learn more about cloud storage in the next section.

Contents

Where's the Cloud?

Even if you haven't been consciously using a cloud storage service, you probably have data stored in the cloud. With many services, you post something or send an e-mail and don't even think about storage. If you use Hotmail, Yahoo or another web-based program, your e-mail history is in the cloud. If you post pictures on Facebook or another social networking site, those images are in the cloud. If you work with others through Google Docs, those documents are in the cloud. If you've posted a video to YouTube, it's in the cloud. If you pay GoDaddy, or a similar company to host your blog, all your blog entries are in the cloud.

We call it the "cloud" because for years, computer professionals have used a cloud icon as shorthand for everything that makes the Internet work – servers, data centers, networks, storage, various services. The cloud is made up of shared resources for us to access through our Internet devices, and we use it on a self-serve basis.

In recent years, as more businesses and individuals see storage as a problem, scores of businesses have sprung up offering to keep data in the cloud for a fee. Some offer a limited amount of storage free, in hopes of gaining your business when you want more.

Essentially, all you need to store data in the cloud is an Internet connection and an arrangement with someone with a server.

You'll want to know more than that about the storage you choose, though. Most cloud systems back up the data they store in multiple computers in multiple locations. That way, if a catastrophe strikes in one place, data is protected elsewhere. Storing data in multiple places is called **redundancy**. Backing up the data you already store in the cloud would add another layer of redundancy that may not be worth the trouble.

Let's look at the pros and cons of cloud storage. Read on to the next section.

Cloud Storage: It's Great, but Not Foolproof

Is cloud storage really all it's cracked up to be?
DANIEL ALLAN/GETTY IMAGES

Let's look at the major advantages and disadvantages of cloud storage. There are lots of arguments in its favor:

- It's easy. You choose a cloud storage provider from the many available, such as Mozy, Carbonite, Dropbox and SugarSync. Install the software and choose which types of documents you want to back up. You may be able to choose the method for encrypting your data for security. Then you just let the service do its job, and you don't have to think about it.
- It can save money. For individuals as well as businesses, cloud storage can be a money saver. You can buy a basic computer model rather than one with lots of storage capacity.
- It can save space.
- It's away from your home and business. If disaster strikes, your data is safe somewhere else.
- You can access your information from any device anywhere you have a good Internet connection. You can also share access with others.
- You can find something on the cloud when you need it more readily than searching through all the discs and folders in your personal archives.

But nothing is foolproof. One big drawback of the cloud is the possibility that your data won't be kept private. If you're wondering whether to back up data that's already in the cloud, you've probably satisfied any doubts you had about security by checking your provider's encryption and authentication practices.

Reliability is another matter. Startup companies sometimes don't last. And devices like Microsoft's Sidekick have had highly publicized failures [source: Dilger]. You never know when and where problems might crop up on the Internet.

Aside from major system failures, data often gets lost in the cloud because of human error or sabotage. For that reason, some people use services like Backupify, which has no delete function, to automatically backup their calendars, pictures, documents, e-mail, social networking accounts and other data in the cloud.

But even if you use Backupify or a similar service, your data is still in the possession of someone else, in the cloud. Is there another approach? And do you need to back up everything some other way?

Read on to the next section for more options – and answers.

Do It Yourself Alternatives

If you're leery of cloud storage providers, or don't want to pay someone else for the service, you can make your own cloud storage system.

A personal cloud is centred on a **network attached storage (NAS) device**. You can buy a hard drive specialized for use as a NAS or adapt an extra computer. Essentially, you're setting up your own private, local data backup and connecting it to the Internet to share as much or as little as you choose.

The advantage to a personal cloud is that everything is under your control and in your possession. Your NAS is in your home or office. You have the one-time cost of the hardware, but no monthly storage fees. You use your own network to access your data anywhere you have an Internet connection.

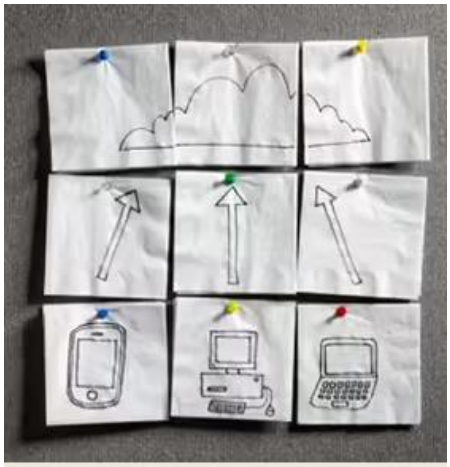
The main disadvantages are what prompt many people to choose cloud storage in the first place: You have to remember to back up your data. You might make a mistake. And if disaster strikes your home or office, you've lost everything.

All storage solutions involving the cloud require a good Internet connection. People who have no Internet connection or weak broadband probably aren't going to find it possible, and certainly not convenient, to use cloud storage. Saving data into the cloud strains a weak Internet connection, and retrieving it would be too time-consuming.

These people must depend on the old-fashioned ways of backing up their data. They can copy it to an external hard drive, a USB (universal serial bus) flash drive or onto CDs, and store it in as safe a place as possible.

People who don't completely trust cloud storage can also resort to such old-fashioned backups.

Is Cloud Storage Safe?



If you want to make sure your data stays safe in the cloud, you may need to do a little research.
JEFFREY COOLIDGE/GETTY IMAGES

That gets us back to the question of whether it's necessary to back up data that's already in the cloud.

At this stage in the evolution of cloud storage, there's no definitive answer to the question of whether it's necessary to back up data that's already in the cloud.

If you've chosen your service provider well, the cloud is most likely going to be at least as safe as and probably more so than anything you devise yourself. Professional companies are in the business to earn money, and their reputation and success depends upon protecting your data.

Another thing to consider about your storage provider is what the fine print in the agreement you sign says about how readily available your data will be. If you need to access it only periodically, you'll probably be fine. Certainly if the data is something you could live without, even if you'd miss it, you can probably skip additional backup. It's highly unlikely that you'll lose your data.

But if you're very cautious, you might want to provide additional back up for any items of absolutely critical data whose loss would cause you severe problems in your business or personal life. You might want to provide your own additional redundancy for them. Back up those especially valuable items up somewhere other than on the cloud, and store them away from your home or office. Just for the peace of mind.

Author's Note

When I started researching this article, I thought it did not apply to me yet, although I might learn something that would change my practices. My first surprise was the realization that through e-mail, social networking and a blog, I am already using cloud data storage.

I learned that cloud computing is rapidly evolving, and that today's best answers might not apply a few years from now.

Probably because things are changing so rapidly, I did not find definitive answers to the question at hand. The general consensus is that for most people and most data, professional cloud storage is at least as safe as the alternatives. I talked to some computer professionals, most of whom were willing to share their opinions but did not want to be cited as sources.

Related Articles

- How Cloud Computing Works
- How Cloud Storage Works

Sources:

- Clark, Andrew. Director of Strategy, IBM Venture Capital Group. Personal interview via e-mail. Sept. 20, 2012.

- Dachis, Adam. "Use Multiple Online Cloud Storage Services for Free and Organized Backup." Lifehacker. (Sept. 15, 2012) http://lifehacker.com/5788508/use-multiple-online-cloud-storage-services-for-free-and-organized-backup
- Dilger, Daniel Eran. Microsoft's Danger Sidekick Loss Casts Dark on Cloud Computing." Apple Insider. Oct. 11, 2009. (Sept. 19 2012) http://appleinsider.com/articles/09/10/11/microsofts_danger_sidekick_data_loss_casts_dark_on_cloud_computing.html
- "Get Your Own Personal Cloud!" Akitio. (Sept. 19, 2012) http://www.akitio.com/information-center/get-your-own-personal-cloud
- "Is it worth backing up to the cloud?" AskJack Blog, The Guardian. (Sept. 15, 2012) http://www.guardian.co.uk/technology/askjack/2012/feb/16/ask-jack-backup-cloud-computing/print.
- Kleyman, Bill. "Creative Ways to Deliver Cloud Computing Services. Data Center Knowledge. (Sept. 14, 2012) http://www.datacenterknowledge.com/archives/2012/09/13/cloud-computing-a-look-at-the-delivery-model/
- Lynn, Samara. "How to Buy a NAS." PC Mag. (Sept. 16, 2012) http://www.pcmag.com/article2/0,2817,2354173,00.asp
- Manjoo, Farhad. "You Should Back Up Your Gmail, Facebook, and Twitter Accounts. Slate.com. Aug. 17, 2012. (Sept. 18, 2012) http://www.slate.com/articles/technology/technology/2012/08/backupify_yes_you_should_back_up_your_gmail_facebook_and_twitter_accounts_here_s_how_to_do_it_.html
- McCabe, Laurie. "What is Cloud Computing and Why Should You Care?" Small Business Computing. March 11, 2009, Updated Oct. 5, 2011. (Sept. 17, 2012) http://www.smallbusinesscomputing.com/biztools/article.php/3809726/What-is-Cloud-Computing--and-Why-Should-You-Care.htm
- Mell, Peter and Timothy Grance. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology, U.S. Department of Commerce. (Sept. 15, 2012) http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- Mozy. "MozyHome Frequently Asked Questions." (Sept. 17, 2012) http://mozy.com/home/faq
- Rodriguez, Andres. "Using the Cloud for Backup: You're Missing the Point." TechNewsWorld. May 10, 2011. (Sept. 15, 2012) http://www.technewsworld.com/story/72421.html
- Thomas, Keir. "Choosing Cloud Backup for PCs." PC World. (Sept. 24, 2012) http://www.pcworld.com/article/223354/choosing_cloud_backup_for_pcs.html
- What Is a NAS and Why Do I Need One?" The Digital Den. Seagate. (Sept. 15, 2012) http://consumer.media.seagate.com/2010/08/the-digital-den/what-is-a-nas-and-why-do-i-need-one/

Frequently Answered Questions

What are the 3 types of backups?

The 3 types of backups are: 1. Full backup 2. Incremental backup 3. Differential backup

5 Tips for Storing and Sharing Photos in the Cloud

By: Nathan Chandler

Cloud photo services mean safer and more secure storage than any hard drive could offer, so you won't have to worry about losing moments like this.
COURTESY 40 NIGHTS PHOTOGRAPHY

The war of the cloud is raging. Don't expect to look into the skies and see a cumulonimbus drawing a lightning sword on an altostratus, though. This cloud war is digital, and the companies who are fighting to fulfill your online data storage needs are targeting one of your most precious belongings -- your massive collection of pictures.

You probably already know that your computer's hard drive isn't the ideal location for your beloved images. For one, hard drives routinely crash, sending the data stored on them into dark oblivion. Furthermore, pictures stored locally often get very little eyeball time, and in today's easy media-sharing environment, there's no reason your photos should be collecting digital dust. The only real question then, is this: What are the best ways to store and share your photos online?

The cloud has all of the answers. When we refer to the **cloud**, we're pointing to online services that store your images in servers that are available from just about any Internet-connected device. For instance, you can upload your pictures from your bulky office desktop PC to online storage and then show those images to a friend at a restaurant via your smartphone.

Cloud photo storage offers a number of tremendous benefits. First, you'll be able to share your pictures just about anytime, anywhere you have Internet access. Second, cloud services routinely back up their data, so you should never permanently lose your priceless and irreplaceable images, even if your own computer explodes into flames.

But balancing the storage and sharing aspects of online images takes a bit of work. With the following tips, you'll reign in the warring cloud factions and use their power for your own photo-tastic ends.

Contents

5: Freebies Can Be Frustrating

There are a lot of options for free online photo storage, but free only takes you so far. With some companies, you'll need to buy prints or other products at least once per year to keep your account active.
COURTESY SHUTTERFLY

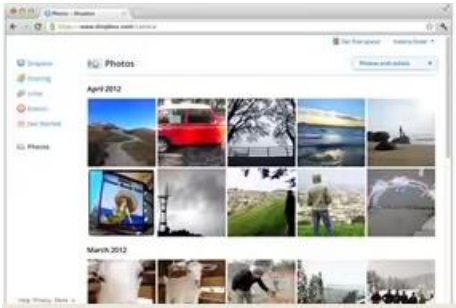
Most cloud services offer free storage to a point, which is often right around 5GB. Once you hit your data cap, though, the attraction of a freebie quickly loses its luster in the face of frustrating limitations.

For example, Internet photo stalwart Flickr does indeed offer free storage. However, you're capped at 300MB of data per month. Depending on the size of the files that your camera creates, that could be fewer than 100 images. Furthermore, Flickr lets you display a maximum of 200 pictures for public viewing. This is just one instance of a company that stunts its free offerings in the hopes that you'll ante up for a paid service.

Yet, if you plan to push your photos into the cloud for years and years, you'll likely wind up opting for a paid account. The good news is that storage pricing is typically very reasonable; the average annual cost for most is well under $100 and often close to $50 or even less.

Still refuse to pay for your photo play? Don't overlook the obvious. Facebook, for example, doesn't restrict the number of images you upload, although it does put a 4MB limit on image size. Sites such as Snapfish and Shutterfly also offer free, unlimited uploads. These services are sometimes tied to products such as prints. SnapFish, for one, requires you to buy products at least once annually to prevent deletion of your images.

4: Automation Nation



Dropbox is one of several services that automatically back up your newest images to online storage, thus eliminating the need to manually upload files.
COURTESY DROPBOX

So you finally decided to pony up for a paid cloud service. You have virtually unlimited storage capacity, easy sharing options and more fun features that you could ever dream of using. Then the almost-unthinkable happens: Your house is flattened by a hurricane, flinging your computer over the horizon. Good thing you have those images backed up online, right? Right?

Only you've been neglecting to drag-and-drop your images to cloud storage for quite some time. Or to be exact, for about 26 months ... the entire lifespan of your toddler. Those 10,000 adorable baby pictures? Poof, gone.

Most people struggle to remember to back up their files. That's why services with automated synchronization and backup options are ideal. Not only do they detect when you've transferred new pictures to your hard drive, but they automatically initiate the upload procedure for you.

Google Drive, SugarSync, CrashPlan and Dropbox are four examples of services that automatically upload your new photos and videos. So if you're the forgetful type, or you tend to procrastinate on backups (and you know who you are), auto-syncing capabilities are a must-have.

3: Care to Share?

Some sites are configured for optimal archiving workflow; others are made to simplify sharing. Be sure the site fits your primary needs before you commit to uploading years' worth of images.
SCREENSHOT BY NATHAN CHANDLER

There's an overabundance of cloud services designed for straight-up data storage. From SkyDrive to Box to Amazon Cloud Drive to Google Drive, you'll never want for a place to park important documents and data files. But not every service lets you share photos with ease.

And sharing, of course, is most of the fun of taking pictures to begin with. Facebook, for example, helps you easily tag friends and locations in your images and notifies your friends when they're tagged. The site's interface doesn't allow for the kind of efficient photo browsing of other services, though.

Dropbox does help you create a link that you can share with your friends. However, that process requires additional work on your part. SkyDrive is one site that automatically plunks uploaded images into a sharable gallery. Google Drive works with the company's Picasa software, and as such, there is no shortage of photo-sharing capabilities.

In summary, most cloud services do offer ways to share images, but you may need to try a two or three before you find a sharing style that works best for you. The best way to find your preferred sharing style? Upload just a few photos to each company and use its service for a few days to see if the interface is friendly, fun and easy to use.

2: Mobile Matters

The mobile photo-sharing market is blowing up. As such, most services now offer a version that works through smartphones.
SCREENSHOT BY NATHAN CHANDLER

With millions of people taking zillions of pictures on their cell phones, cloud services are making moves to satisfy the demands of mobile. In some cases, the kind of phone you use will influence your mobile cloud options.

If you own a Windows Phone, for instance, your images can be automatically synced to your Microsoft SkyDrive. And your Android phone (powered by Google's Android operating system) will easily help you sync to a Google Drive. Have an iPhone? You can funnel your images straight to Apple's iCloud.

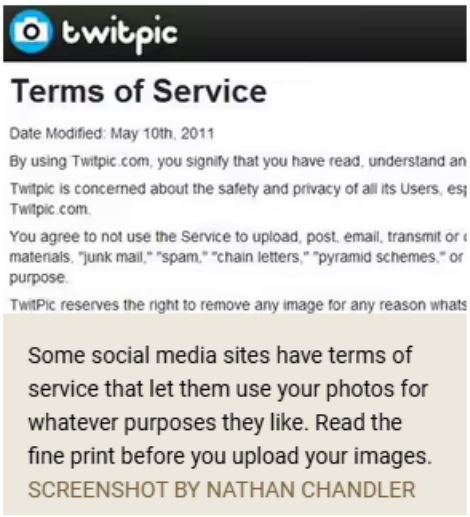
On the flip side, SkyDrive won't let you use an Android phone. DropBox nixes Windows Phone, and Google Drive doesn't allow iOS devices or Windows Phone yet. Amazon Cloud Drive and Apple iCloud, though, couldn't care less what mobile device you're using.

No matter which phone you use, you have access to a range of photo-sharing apps. And although its mobile app gets plenty of criticism, Facebook's ubiquity and many options make it a solid option. You can even tag images quickly, no matter where you are.

Two caveats with mobile photos – understand your phone's data plan. Because photo upload and downloads consume a lot of data, you might quickly run up against data restrictions or exorbitant, especially if you have your phone set to auto-sync every photo you capture.

Also remember that you don't have to use the highest-resolution setting on your phone's camera. An 8-megapixel picture takes way more storage and bandwidth than a 2-megapixel file, so unless you're making really large hardcopy prints from your files, bigger is definitely not better.

1: Your Rights Fight



If there's one thing to remember about online photo sharing and storage, it's this: The services and options change as quickly as the weather. So, too, do their terms of service, which can be a sticky, confusing mess that results in other people using your pictures for their own profit.

Understand that more than a few social media sites (such as TwitPic and Instagram) make picture sharing very simple and fun. But use these services with this caveat -- you may be giving that site permission to use or distribute your pictures in any way they see fit.

Protect yourself by reading the terms of service or by searching for TOS complaints regarding specific sites. One upside is that these sorts of TOSes are more common with social-media sites than storage-centric services.

Finally, keep in mind that there isn't a one-size-fits-all photo storage and sharing system. Your needs may even change depending on the project. To wit: Facebook is great for random snapshots, but Flickr is sleeker and slicker for a burgeoning album of vacation photos.

No matter which road you take to the cloud, you should be excited for the future of digital photo fun. As these services expand and companies tweak their business models, your options will continue to increase exponentially.

Lots More Information

Author's Note

This is truly a golden age in the era of digital photography. The technology just keeps getting better, cheaper and more innovative -- to the point where there are so many options and capabilities that your imagination is the only limiting factor.

The same goes for storing and sharing your images through the cloud. Now your images can be at your fingertips, anywhere you can find a 3G or WiFi signal. The potential for communicating your ideas and your vision of the world is now just a touchscreen away, no matter where you happen to be.

Not only are your sacred family images safer than ever before, but more and more people have the opportunity to see them. These days, there really is no reason that grandma can't see pictures of the new baby, updated daily, or even on the hour, for years to come.

Related Articles

- Are my files really safe if I store them in the cloud?
- How the Google Cloud Works
- How Cloud Computing Works

- How Cloud Storage Works
- 5 Tools for Digital Photo Albums

Sources

- **Bradley, Tony. "The Cloud, Day 13: Storing and Managing Pictures in the Cloud." PCworld.com. Nov. 26, 2011. (June 14, 2012) http://www.pcworld.com/businesscenter/article/244949/the_cloud_day_13_storing_and_managing_pictures_in_the_cloud.html**
- **DesMaraias, Christina. "The Cloud Gets More Awesome with New Offers." PCworld.com. Feb. 25, 2012. (June 14, 2012) http://www.pcworld.com/article/250699/the_cloud_gets_more_awesome_with_new_offers.html**
- **Gordon, Whitson. "Cubby is Like Dropbox...If Dropbox also had Free, Unlimited Syncing." Lifehacker.com. May 11, 2012. (June 14, 2012) http://lifehacker.com/5907654/cubby-is-like-dropbox-if-dropbox-also-had-free-unlimited-syncing-and-weve-got-invites?tag=cloudstorage**
- **Jesdanun, Anick. "Review: Which Cloud Storage Site is Right for You?" USA Today. May 4, 2012. (June 14, 2012) http://www.usatoday.com/tech/products/story/2012-05-05/cloud-storage-review/54748762/1**
- **Johnson, Dave. "Best Ways to Share Photos: Top Sharing Sites, Cloud Services, and more." PCworld.com. Dec. 26, 2011. (June 14, 2012) http://www.pcworld.com/article/246993/best_ways_to_share_photos_top_sharing_sites_cloud_services_and_more.html**
- **Kantra, Suzanne. "Is Cloud Storage Safe for your Kids' Photos?" USA Today. April 27, 2012. (June 14, 2012) http://www.usatoday.com/tech/products/story/2012-04-28/techlicious-cloud-photo-storage/54581314/1**
- **Magennis, Niall. "Best Cloud Services for Email, Movies, Music and More." CNET. April 5, 2012. (June 14, 2012) http://reviews.cnet.co.uk/software-and-web-apps/best-cloud-services-for-email-movies-music-and-more-50007552/**
- **Newman, Jared. "How to Choose Between Cloud Storage Services Like Google Drive and Dropbox." Time Magazine Techland Blog. April 27, 2012. (June 14, 2012) http://techland.time.com/2012/04/27/how-to-choose-between-cloud-storage-services-like-google-drive-and-dropbox/**
- **Pinola, Melanie. "What Cool Things can I do with All This Free Cloud Storage Space?" Lifehacker.com. May 17, 2012. (June 14, 2012) http://lifehacker.com/cloud-storage/**
- **Pinola, Melanie. "Upgrade from 7GB to 25GB of Free Microsoft SkyDrive Storage while you can." Lifehacker.com. April 25, 2012. (June 14, 2012) http://lifehacker.com/5905111/upgrade-from-7gb-to-25gb-of-free-microsoft-skydrive-storage?tag=cloudstorage**
- **Rose, Brent. "The Best Way to Store Stuff in the Cloud." Gizmodo.com. Sept. 28, 2011. (June 14, 2012) http://gizmodo.com/5828035/the-best-way-to-store-stuff-in-the-cloud**

- **Shih, Gary. "Dropbox Heats up Cloud Battle with Photo Upload Feature." Reuters. Feb. 24, 2012. (June 14, 2012) http://www.reuters.com/article/2012/02/24/us-dropbox-photos-idUSTRE81N0BZ20120224**
- **Sung, Dan. "Apple iCloud vs. Google vs. Amazon Cloud Drive vs. DropBox vs. Microsoft SkyDrive." Pocket-lint.com. (June 14, 2012) http://www.pocket-lint.com/news/40364/icloud-google-music-dropbox-skydrive-amazon-cloud-player**

Are my files really safe if I store them in the cloud?

By: Stephanie Crawford

Storing your data on cloud servers is easier than ever -- many services offer drag-and-drop interfaces or seamless automatic backup. Be sure you're handling your files mindfully.
©ISTOCKPHOTO.COM/ALEXSL

The days of keeping all your documents, photos and music on your computer's hard drive are gradually coming to a close. Today, cloud storage is helping to solve the ever-present need for more storage space to hold all of your digital property. But is all your personal data safe out there on the Internet?

To answer this question, we need to examine two things. First, we need to decide what constitutes data security. Is password access to the storage sufficient, or should files be fully encrypted on the storage device? Some of that will be up to you, but everyone should note these important security points:

- Passwords can be hacked. This doesn't mean that passwords aren't safe, just that they're vulnerable to dictionary and brute force attacks, as described in our article How Hackers Work. If you choose a cloud storage solution that relies on a password to access your data, choose a password that's difficult to hack with dictionary attacks, and change your password often to reduce the chances of success from brute force attacks.

- Passwords can be hacked. This doesn't mean that passwords aren't safe, just that they're vulnerable to dictionary and brute force attacks, as described in our article How Hackers Work. If you choose a cloud storage solution that relies on a password to access your data, choose a password that's difficult to hack with dictionary attacks, and change your password often to reduce the chances of success from brute force attacks.

- Data can be captured en route. Fortunately, most storage services will encrypt the data while it's traveling back and forth, making it impossible to read even if someone captures the files. If your cloud storage works through a Web app, look for "https" instead of "http" in front of the URL in your browser's address bar. That extra "s" indicates the form is using secure HTTP. If you have a standalone cloud storage app installed on your computer, check to be sure that app uses some type of encryption for its Internet exchanges.
- People are more dangerous than computers when it comes to hacking. Don't give out your password to anyone, even someone claiming to be from technical support. One of the biggest dangers for security is social engineering: creating a trust between the hacker and the end user that causes the end user to happily hand over personal information. Note that

when you speak with the real technical support specialists, they'll require only minimal identifying information from you, and most likely not your password.

- Hackers usually want the most information for the least effort. This means they will likely attack the heart of a cloud storage service rather than its individual users. Thus, you probably want to find a service provider with a good history of keeping its clients' accounts and data secure.
- Your data isn't always immune to search and seizure by local government entities. In the U.S., for example, any cloud storage company could be served a subpoena requiring them to open their clients' data for government examination.

We also need to look at cloud storage providers to see which ones are doing the most to keep your information safe. Next, let's look at how the major cloud storage providers protect data and go over some tips for choosing a safe cloud storage service.

Safe Cloud Storage Options

When you're shopping for a cloud storage service for your files, you'll probably start by considering what you plan to store and how you need to access it. Along with that, determine how important it is to keep that information secure. For example, if you're storing important documents about your medical history or home finances, you may be more concerned about keeping your data safe than you would, say, music files from CDs you've ripped. Here are some safety features to look for when you're shopping:

- A company with a reputation for excellent physical and network security
- Multiple-level redundancy, meaning there are multiple copies of your data to prevent loss in the case of a single disk or server failure
- Redundancy across multiple geographic locations, so when a natural disaster destroys your data at one location, that same data is still available elsewhere
- How long it takes to delete a file across the redundant servers in the cloud, or if it's ever truly deleted from the cloud storage banks

Cloud security hasn't been as rigid for end-user storage services as it has for enterprise-level clouds. As a result, even the top cloud storage options available to you have some vulnerabilities. While these vulnerabilities are probably not a big concern for most users, they are worth noting if you decide to store sensitive personal information. The following are just a couple of examples:

Dropbox -- Dropbox is simple and sufficient for most users, encrypting your data while it's in transit over the Internet. In its simplicity, though, it did leave a couple of security holes. First, it left local authentication protection up to its users. All you need to sign in from another computer is a copy of your Dropbox configuration file, so you're responsible for limiting access to your local computer. Dropbox also leaves the names of your files in plain text. It's up to you whether you want a third-party security application to encrypt and decrypt the data in the folder you're synchronizing locally to protect filenames and prevent anyone from reading that data without your additional decryption keys [sources: G.F., Newton].

Amazon Cloud Drive -- Amazon stands toe-to-toe with Dropbox when it comes to simplicity and availability across platforms. Amazon is also up front about one of your security risks. In its user agreement, Amazon Cloud Drive declares its right to access your files and disclose account

information to offer support and to ensure compliance with that agreement. Since the Cloud Drive offers streaming of MP3, this is largely to enforce copyright law regarding music. If you want to protect those files, you'll have to give up the streaming option for media files and use a third-party encryption app for all the data you synchronize to the Cloud Drive [sources: Vaughan-Nichols, Raphael].

So, our answer to the title question for this article is this: Yes, but know the limitations of your cloud storage service before you start uploading. For more information on cloud security, head on to the next page.

Lots More Information

Related Articles

- How Cloud Computing Works
- How Apple iCloud Works
- How the Amazon Cloud Player Works
- How Hackers Work
- 5 Apps to Organize Your Life
- 10 iPad Apps for Personal Productivity

More Great Links

- Seven cloud-computing security risks

Sources

- **Bradley, Tony. "iCloud Raises Serious Data Security Concerns." PCWorld. PCWorld Communications, Inc. Jun. 8, 2011. (Sep. 7, 2011) http://www.pcworld.com/businesscenter/article/229823/icloud_raises_serious_data_security_concerns.html**
- **G.F. "Internet security: Keys to the cloud castle." The Economist. The Economist Newspaper Limited. May 18, 2011. (Sep. 7, 2011) http://www.economist.com/blogs/babbage/2011/05/internet_security**
- **Newton, Derek. "Dropbox authentication: insecure by design." Blog: Information Security Insights. Apr. 2011. (Sep. 7, 2011) http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/**
- **Raphael, J.R. "Amazon Cloud Drive: 3 things to consider before you commit." Computerworld, Inc. Mar. 30, 2011. (Sep. 7, 2011) http://blogs.computerworld.com/18056/amazon_cloud_drive**
- **Rothman, Rachel. "Cloud Computing: Safe Data Storage." Good Housekeeping. Hearst Communications, Inc. Mar. 28, 2011. (Sep. 7, 2011) http://www.goodhousekeeping.com/product-testing/from-the-lab-blog/Cloud-Computing**
- **Vaughan-Nichols, Steven J. "No Privacy on Amazon's Cloud Drive." ZDNet. CBS Interactive. Mar. 29, 2011. (Sep. 7, 2011) http://www.zdnet.com/blog/networking/no-privacy-on-amazons-cloud-drive/882**

Should I move my hard disk to the cloud?

By: Jonathan Strickland

Is your data better off in the cloud than on a hard disk drive like this one? PHOTODISC/THINKSTOCK

Whether you have a terabyte worth of vacation photos or a host of sensitive documents sitting on your computer, you want to keep your data safe, secure and accessible. A big part of achieving these goals is choosing where your data will live. Should you rely on your computer's hard drive? Is an external hard drive for backup purposes necessary? Or should you shift all your data to the cloud?

Cloud storage has been making headlines for a few years now. The concept is pretty simple. You access the service through an Internet-connected device, pulling up whichever files you need at the time. Those files reside on servers that could potentially be thousands of miles or kilometers away.

There are dozens of companies that offer some form of cloud storage. Some even allot users a certain amount of storage space for free. With all the competition in the market, customers can shop around for the deal that makes the most sense for them. All of this is good news for people interested in cloud storage, but is it actually a good idea?

Let's take a look at the pros and cons of cloud storage and why backing up your data is critical.

Contents

Silver Linings in Clouds

Perhaps the most attractive feature of cloud storage is that it gives you lots of options when it comes to retrieving your data. Typically, cloud storage services require that you create a password-protected account with a unique user name. Logging into the service through a desktop program, smartphone app or Web browser gives you access to your files.

That means you don't have to keep track of various drives or devices. You can open a file on one computer, make some changes and save it to the cloud. Later, you can access the new version of the file on a different computer by logging into the cloud service. There's no need to e-mail files or save them to a physical medium like a flash drive.

Another positive feature of cloud computers is that any reputable service will ensure redundancy by storing your data on multiple servers. That way, should one server suffer a failure, you'll still be able to access your personal files without interruption. Most cloud networks have computers that take on the task of making sure every server holding your data has the latest version of the file.

Have you ever lost a digital file or had a hard drive go bad? It can be a stressful experience. You may have to bring a hard drive or computer to a data retrieval specialist and even then you may not get

everything back. That's why backing up your data is important. It creates redundancy -- should one drive fail, you can still access the data on another system. Whether you prefer cloud storage or an external drive in your possession, consider backing up your data. It has the potential to prevent a huge headache.

Storing your data in the cloud also protects your information in case something should happen to your physical machine. Disasters like floods or fires could destroy all your information. A good cloud storage network will house servers in a secure location with failsafe systems in place to protect the machines.

Chromed Out

Google's Chromebook computers are designed to work with documents stored in the cloud. The computers don't need to be particularly powerful or have a lot of storage -- the cloud does all the heavy lifting.

Stormy Clouds

Is your data better off in the cloud than on a hard disk drive like this one? ISTOCKPHOTO/THINKSTOCK

There are some drawbacks to cloud storage as well. Cloud storage is a business and businesses can fail. If the cloud storage system you use has financial trouble, you may find yourself in the position of retrieving all your data in a short amount of time before the service goes offline. It also means trusting that the failing business will take every measure to ensure all customer data gets wiped out before selling off assets -- you wouldn't want your personal files to end up on a server sold to some other company.

If you're concerned about privacy, it's also good to look into how your data could be used by the service. This means reading the **terms of service** -- that long document that people often skim over before clicking on "Agree." It's possible some cloud storage services could send you targeted advertising based upon the files you save within the system. It may be that no human being is reading your information, but for some people the thought of a system mining files for advertising purposes is a deal breaker.

One question you should ask before diving into a cloud storage service is "Who owns my data?" Again, reading the terms of service is crucial. Some services may indicate that the service effectively owns anything you store on its servers. While it's clear that you own your data when you store it on a local hard drive, the same may not be true when you use cloud storage.

There's also the issue of data security. A good cloud storage service will encrypt all data. Ideally, the data will remain unusable even should a hacker gain access to it. It's safe to bet that the larger cloud service companies employ security measures far more strict than the average computer owner. But it's also true that these companies are bigger targets than the typical user.

One last drawback is that you need an Internet connection to access your files. If you happen to be in a place that has limited or no access to the Internet or should your Internet service fail, your data will remain out of reach. The same is true if there is a catastrophic failure at the cloud service facility -- should the data center lose power or connectivity, your data will be out of reach.

Remember, it's in the cloud storage service's best interest to make sure connectivity and security are as strong as possible. But it remains true that you need to take these factors into consideration before making a move to the cloud.

Ultimately, the important note to take away from this is that you should backup your data. Don't store all your digital information on a single device -- devices fail and you may lose something important or irreplaceable. A balance of local and cloud storage can be a great solution. Just be sure to research the cloud storage services you're considering to make sure they're a good fit!

Author's Note

I use a combination of local and cloud storage to store my files. I have an external hard drive that my iMac uses as a backup every week. I use cloud storage for many of my personal projects. I even have a dozen or so thumb drives I use to store photos, videos and other files. Keeping track of all the various forms of storage is in itself complicated but it helps keep my data safe through redundancy.

Related Articles

- How Cloud Storage Works
- How Hard Disks Work
- Are my files really safe if I store them in the cloud?
- How Cloud Computing Works
- How the Google Cloud Works

Sources

- Baylor University. "Cloud Services." (Sept. 4, 2012) http://www.baylor.edu/its/index.php?id=86451
- Lata, Mike. "Google Drive, Dropbox, iCloud: Data Privacy in the Public Cloud." TrainSignal. May 8, 2012 (Sep 4, 2012) http://www.trainsignal.com/blog/public-cloud-storage-privacy
- Srivastava, Mandira. "Cloud Computing – The Risks and Benefits of Cloud Storage." Smallbiz Technology. Sept. 12, 2011. (Sept. 4, 2012) http://www.smallbiztechnology.com/archive/2011/09/cloud-computing-the-risks-and-benefits-of-cloud-storage.html/
- Vaas, Lisa. "Cloud Storage Security Isn't as Solid as Vendors Want You to Believe." eWeek. May 15, 2012. (Sept. 4, 2012). http://www.eweek.com/c/a/Security/Cloud-Storage-Security-Isnt-as-Solid-as-Vendors-Want-You-to-Believe-248889/

What is Cloud Storage?

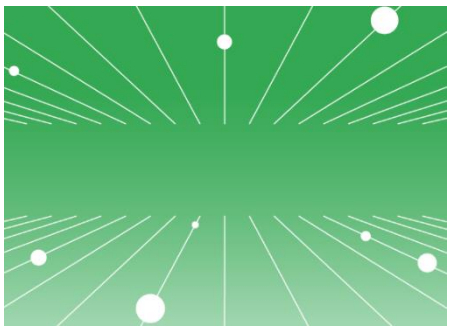
Cloud Storage is a mode of computer data storage in which digital data is stored on servers in off-site locations. The servers are maintained by a third-party provider who is responsible for hosting, managing, and securing data stored on its infrastructure. The provider ensures that data on its servers is always accessible via public or private internet connections.

Cloud Storage enables organizations to store, access, and maintain data so that they do not need to own and operate their own data centers, moving expenses from a capital expenditure model to operational. Cloud Storage is scalable, allowing organizations to expand or reduce their data footprint depending on need.

Google Cloud provides a variety of scalable options for organizations to store their data in the cloud. Learn more about Cloud Storage at Google Cloud.

Get started for free

Learn about Cloud Storage



Watch on-demand

What's new and next: a spotlight on storage

How does Cloud Storage work?

Cloud Storage uses remote servers to save data, such as files, business data, videos, or images. Users upload data to servers via an internet connection, where it is saved on a virtual machine on a physical server. To maintain availability and provide redundancy, cloud providers will often spread data to multiple virtual machines in data centers located across the world. If storage needs increase, the cloud provider will spin up more virtual machines to handle the load. Users can access data in Cloud Storage through an internet connection and software such as web portal, browser, or mobile app via an application programming interface (API).

Cloud Storage is available in four different models:

Public

Public Cloud Storage is a model where an organization stores data in a service provider's data centers that are also utilized by other companies. Data in public Cloud Storage is spread across multiple regions and is often offered on a subscription or pay-as-you-go basis. Public Cloud Storage is considered to be "elastic" which means that the data stored can be scaled up or down depending on the needs of the organization. Public cloud providers typically make data available from any device such as a smartphone or web portal.

Private

Private Cloud Storage is a model where an organization utilizes its own servers and data centers to store data within their own network. Alternatively, organizations can deal with cloud service providers to provide dedicated servers and private connections that are not shared by any other organization. Private clouds are typically utilized by organizations that require more control over their data and have stringent compliance and security requirements.

Hybrid

A hybrid cloud model is a mix of private and public cloud storage models. A hybrid cloud storage model allows organizations to decide which data it wants to store in which cloud. Sensitive data and data that must meet strict compliance requirements may be stored in a private cloud while less sensitive data is stored in the public cloud. A hybrid cloud storage model typically has a layer of orchestration to integrate between the two clouds. A hybrid cloud offers flexibility and allows organizations to still scale up with the public cloud if need arises.

Multicloud

A multicloud storage model is when an organization sets up more than one cloud model from more than one cloud service provider (public or private). Organizations might choose a multicloud model if one cloud vendor offers certain proprietary apps, an organization requires data to be stored in a specific country, various teams are trained on different clouds, or the organization needs to serve different requirements that are not stated in the servicers' Service Level Agreements. A multicloud model offers organizations flexibility and redundancy.

Advantages of Cloud Storage

Total cost of ownership

Cloud Storage enables organizations to move from a capital expenditure to an operational expenditure model, allowing them to adjust budgets and resources quickly.

Elasticity

Cloud Storage is elastic and scalable, meaning that it can be scaled up (more storage added) or down (less storage needed) depending on the organization's needs.

Flexibility

Cloud Storage offers organizations flexibility on how to store and access data, deploy and budget resources, and architect their IT infrastructure.

Security

Most cloud providers offer robust security, including physical security at data centers and cutting edge security at the software and application levels. The best cloud providers offer zero trust architecture, identity and access management, and encryption.

Sustainability

One of the greatest costs when operating on-premises data centers is the overhead of energy consumption. The best cloud providers operate on sustainable energy through renewable resources.

Redundancy

Redundancy (replicating data on multiple servers in different locations) is an inherent trait in public clouds, allowing organizations to recover from disasters while maintaining business continuity.

Disadvantages of Cloud Storage

Compliance

Certain industries such as finance and healthcare have stringent requirements about how data is stored and accessed. Some public cloud providers offer tools to maintain compliance with applicable rules and regulations.

Latency

Traffic to and from the cloud can be delayed because of network traffic congestion or slow internet connections.

Control

Storing data in public clouds relinquishes some control over access and management of that data, entrusting that the cloud service provider will always be able to make that data available and maintain its systems and security.

Outages

While public cloud providers aim to ensure continuous availability, outages sometimes do occur, making stored data unavailable.

How to use Cloud Storage

Cloud Storage provides several use cases that can benefit individuals and organizations. Whether a person is storing their family budget on a spreadsheet, or a massive organization is saving years of financial data in a highly secure database, Cloud Storage can be used for saving digital data of all kinds for as long as needed.

Backup

Data backup is one of the simplest and most prominent uses of Cloud Storage. Production data can be separated from backup data, creating a gap between the two that protects organizations in the case of a cyber threat such as ransomware. Data backup through Cloud Storage can be as simple as saving files to a digital folder such as Google Drive or using block storage to maintain gigabytes or more of important business data.

Archiving

The ability to archive old data has become an important aspect of Cloud Storage, as organizations move to digitize decades of old records, as well as hold on to records for governance and compliance purposes. Google Cloud offers several tiers of storage for archiving data, including coldline storage and archival storage, that can be accessed whenever an organization needs them.

Disaster recovery

A disaster—natural or otherwise— that wipes out a data center or old physical records needs not be the business-crippling event that it was in the past. Cloud Storage allows for disaster recovery so that organizations can continue with their business, even when times are tough.

Data processing

As Cloud Storage makes digital data immediately available, data becomes much more useful on an ongoing basis. Data processing, such as analyzing data for business intelligence or applying machine learning and artificial intelligence to large datasets, is possible because of Cloud Storage.

Content delivery

With the ability to save copies of media data, such as large audio and video files, on servers dispersed across the globe, media and entertainment companies can serve their audience low-latency, always available content from wherever they reside.

Types of Cloud Storage

Cloud Storage comes in three different types: **object**, **file**, and **block**.

Object

Object storage is a data storage architecture for large stores of unstructured data. It designates each piece of data as an object, keeps it in a separate storehouse, and bundles it with metadata and a unique identifier for easy access and retrieval.

File

File storage organizes data in a hierarchical format of files and folders. File storage is common in personal computing where data is saved as files and those files are organized in folders. File storage makes it easy to locate and retrieve individual data items when they are needed. File storage is most often used in directories and data repositories.

Block

Block storage breaks data into blocks, each with an unique identifier, and then stores those blocks as separate pieces on the server. The cloud network stores those blocks wherever it is most efficient for the system. Block storage is best used for large volumes of data that require low latency such as workloads that require high performance or databases.

Related products and services

Google Cloud offers a variety of products and services to help organizations make the most of cloud storage.

By using Google Cloud, organizations are using the most sustainable cloud in the business, with the most robust artificial intelligence and machine learning solutions.

Google Workspace

A flexible, innovative solution for people and organizations to achieve more.

Persistent Disk storage

Reliable, high-performance block storage for virtual machine instances.

Filestore

High-performance, fully managed file storage.

Storage Transfer Service

Transfer data quickly and securely between object and file storage across Google Cloud, Amazon, Azure, on-premises, and more.

Artifact Registry

The next generation of Container Registry. Store, manage, and secure your build artifacts.

Solution

Data lake modernization

Google Cloud's data lake powers any analysis on any type of data. This empowers your teams to securely and cost-effectively ingest, store, and analyze large volumes of diverse, full-fidelity data.

Solution

Data center migration

Whether you need to exit or reduce on-premises data centers, migrate workloads as is, modernize apps, or leave another cloud, we'll work together to craft the right cloud migration solutions for you and your business.

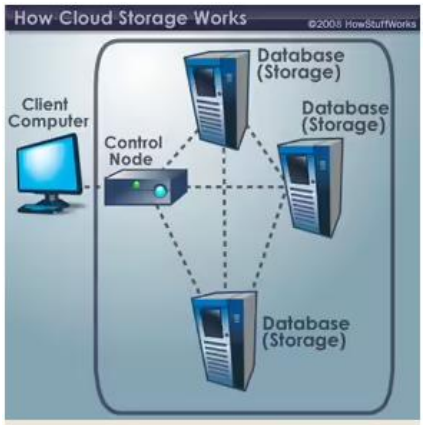
Take the next step

Start building on Google Cloud with $300 in free credits and 20+ always free products.

Get started for free

How Cloud Storage Works

By: Jonathan Strickland



A typical cloud storage system architecture includes a master control server and several storage servers.
HOWSTUFFWORKS 2008

Comedian George Carlin has a routine in which he talks about how humans seem to spend their lives accumulating "stuff." Once they've gathered enough stuff, they have to find places to store all of it. If Carlin were to update that routine today, he could make the same observation about computer information. It seems that everyone with a computer spends a lot of time acquiring data and then trying to find a way to store it.

For some computer owners, finding enough storage space to hold all the data they've acquired is a real challenge. Some people invest in larger hard drives. Others prefer external storage devices like thumb drives or compact discs. Desperate computer owners might delete entire folders worth of old files in order to make space for new information. But some are choosing to rely on a growing trend: **cloud storage**.

While cloud storage sounds like it has something to do with weather fronts and storm systems, it really refers to saving data to an off-site storage system maintained by a third party. Instead of storing information to your computer's hard drive or other local storage device, you save it to a remote database. The Internet provides the connection between your computer and the database.

On the surface, cloud storage has several advantages over traditional data storage. For example, if you store your data on a cloud storage system, you'll be able to get to that data from any location that has Internet access. You wouldn't need to carry around a physical storage device or use the same computer to save and retrieve your information. With the right storage system, you could even allow other people to access the data, turning a personal project into a collaborative effort.

So cloud storage is convenient and offers more flexibility, but how does it work? Find out in the next section.

Owning Up

One issue that information experts, computer scientists and entrepreneurs debate is the concept of data ownership. Who owns the data stored in a cloud system? Does it belong to the client who originally saved the data to the hardware? Does it belong to the company that owns the physical equipment storing the data? What happens if a client goes out of business? Can a cloud storage host delete the former client's data? Opinions vary on these issues.

Contents

Cloud Storage Basics

There are hundreds of different cloud storage systems. Some have a very specific focus, such as storing Web e-mail messages or digital pictures. Others are available to store all forms of digital data. Some cloud storage systems are small operations, while others are so large that the physical equipment can fill up an entire warehouse. The facilities that house cloud storage systems are called **data centers**.

At its most basic level, a cloud storage system needs just one data server connected to the Internet. A client (e.g., a computer user subscribing to a cloud storage service) sends copies of files over the Internet to the data server, which then records the information. When the client wishes to retrieve the information, he or she accesses the data server through a Web-based interface. The server then either sends the files back to the client or allows the client to access and manipulate the files on the server itself.

Cloud storage systems generally rely on hundreds of data servers. Because computers occasionally require maintenance or repair, it's important to store the same information on multiple machines. This is called **redundancy**. Without redundancy, a cloud storage system couldn't ensure clients that they could access their information at any given time. Most systems store the same data on servers that use different power supplies. That way, clients can access their data even if one power supply fails.

Not all cloud storage clients are worried about running out of storage space. They use cloud storage as a way to create backups of data. If something happens to the client's computer system, the data survives off-site. It's a digital-age variation of "don't put all your eggs in one basket."

What are some examples of cloud storage systems? Keep reading to find out.

Castle in the Clouds

Cloud storage is a subcategory of **cloud computing**. Cloud computing systems offer users access to not only storage, but also processing power and computer applications installed on a remote network.

Examples of Cloud Storage

These servers store Electronic Health Records (EHR) for the Military Health System, allowing doctors to access health records of patients instantly.
DAVID S. HOLLOWAY/GETTY IMAGES

There are hundreds of cloud storage providers on the Web, and their numbers seem to increase every day. Not only are there a lot of companies competing to provide storage, but also the amount of storage each company offers to clients seems to grow regularly.

You're probably familiar with several providers of cloud storage services, though you might not think of them in that way. Here are a few well-known companies that offer some form of cloud storage:

- Google Docs allows users to upload documents, spreadsheets and presentations to Google's data servers. Users can edit files using a Google application. Users can also publish documents so that other people can read them or even make edits, which means Google Docs is also an example of cloud computing.
- Web e-mail providers like Gmail, Hotmail and Yahoo! Mail store e-mail messages on their own servers. Users can access their e-mail from computers and other devices connected to the Internet.
- Sites like Flickr and Picasa host millions of digital photographs. Their users create online photo albums by uploading pictures directly to the services' servers.
- Web site hosting companies like StartLogic, Hostmonster and GoDaddy store the files and data for client Web sites.
- Social networking sites like Facebook and MySpace allow members to post pictures and other content. All of that content is stored on the respective site's servers.
- Services like Xdrive, MediaMax and Strongspace offer storage space for any kind of digital data.

Some of the services listed above are free. Others charge a flat fee for a certain amount of storage, and still others have a sliding scale depending on what the client needs. In general, the price for online storage has fallen as more companies have entered the industry. Even many of the companies that charge for digital storage offer at least a certain amount for free.

Is there enough of a demand for storage to support all the companies jumping into the market? Some people think that if there's space to be filled, someone will fill it. Others think the industry is

destined to experience a crash not unlike the dot-com bubble burst in 2000. We'll have to wait and see.

What are some potential cloud storage problems? Find out in the next section.

A Storm's Brewing

Some people envision a future in which the entire Web becomes a massive storage cloud. People will constantly upload and download data to and from the cloud. The concept of data ownership will lose its meaning. Everyone will have access to everything and secrecy will cease to exist. Other people dismiss these ideas and say that cloud storage is just a tool like any other, and while some might use it to great advantage, it won't bring about the end of civilization as we know it. Who's right? We'll just have to wait and see.

Concerns about Cloud Storage

The two biggest concerns about cloud storage are **reliability** and **security**. Clients aren't likely to entrust their data to another company without a guarantee that they'll be able to access their information whenever they want and no one else will be able to get at it.

To secure data, most systems use a combination of techniques, including:

- **Encryption**, which means they use a complex **algorithm** to encode information. To decode the encrypted files, a user needs the encryption key. While it's possible to crack encrypted information, most hackers don't have access to the amount of computer processing power they would need to decrypt information.
- **Authentication** processes, which require to create a user name and password.
- **Authorization** practices -- the client lists the people who are authorized to access information stored on the cloud system. Many corporations have multiple levels of authorization. For example, a front-line employee might have very limited access to data stored on a cloud system, while the head of human resources might have extensive access to files.

Even with these protective measures in place, many people worry that data saved on a remote storage system is vulnerable. There's always the possibility that a hacker will find an electronic back door and access data. Hackers could also attempt to steal the physical machines on which data are stored. A disgruntled employee could alter or destroy data using his or her authenticated user name and password. Cloud storage companies invest a lot of money in security measures in order to limit the possibility of data theft or corruption.

The other big concern, reliability, is just as important as security. An unstable cloud storage system is a liability. No one wants to save data to a failure-prone system, nor do they want to trust a company that isn't financially stable. While most cloud storage systems try to address this concern through redundancy techniques, there's still the possibility that an entire system could crash and leave clients with no way to access their saved data.

Cloud storage companies live and die by their reputations. It's in each company's best interests to provide the most secure and reliable service possible. If a company can't meet these basic client expectations, it doesn't have much of a chance -- there are too many other options available on the market.

To learn more about cloud storage systems and related topics, follow the links on the next page.

Data Center Design

- Physical security is just as important as network security. Data servers are valuable not only because the machines themselves are expensive, but also because the data stored on them could include sensitive information. Malicious hackers don't rely solely on cracking into a computer system electronically -- sometimes they try to infiltrate a system by gaining access to its physical computers.
- A single data server's power requirements aren't very taxing. But when a data center has hundreds of servers, it's crucial that the center's electric wiring can support the workload.
- Like all computers, data servers generate heat. Too much heat can impair or damage servers, so the data center needs an effective cooling system to prevent such problems.

Read More

Lots More Information

Related HowStuffWorks Articles

- How Cloud Computing Works
- How Shared Computing Works
- How the Google Apple Cloud Computer Will Work
- How Quantum Computers Will Work
- How Web Servers Work
- How Encryption Works
- How Hackers Work
- How Home Networking Works
- How Internet Infrastructure Works
- How Internet Search Engines Work
- How Microprocessors Work
- How Semantic Web Works
- How Web Pages Work

More Great Links

- The Globus Alliance
- Grid Computing Info Centre
- Grid Computing Planet
- IBM Grid computing
- Open Grid Forum

Sources

- **Brodkin, Jon. "IBM unveils 'cloud computing.'" Network World. Nov. 19, 2007. Vol. 24, Iss. 45. pg. 10.**
- **Cheng, Jacqui. "Google, Microsoft and Apple building online storage havens: you win." Ars technica. August 12, 2007. Retrieved March 18, 2007. http://arstechnica.com/news.ars/post/20070812-google-microsoft-and-apple-building-online-storage-havens-you-win.html**
- **Hickins, Michael. "Cloud Computing Gets Down to Earth." eWeek. January 21, 2008. pg. 14.**
- **"IBM Introduces Ready-to-Use Cloud Computing." IBM. Nov. 15, 2007. http://www-03.ibm.com/press/us/en/pressrelease/22613.wss**
- **Lohr, Steve. "Cloud Computing and EMC Deal." The New York Times. Feb. 25, 2008. pg. C 6.**
- **Lohr, Steve. "Google and I.B.M. Jon in 'Cloud Computing' Research." The New York Times. Oct. 8, 2007. pg. C 8.**
- **Lohr, Steve. "I.B.M. to Push 'Cloud Computing,' Using Data From Afar." The New York Times. Nov. 15, 2007. pg. C 7.**
- **Markoff, John. "Software via the Internet: Microsoft in 'Cloud' Computing." The New York Times. Sep. 3, 2007. pg. C 1.**
- **Naone, Erica. "Computer in the Cloud." Technology Review. Sept. 18, 2007. Retrieved March 12, 2008. http://www.technologyreview.com/Infotech/19397/?a=f**
- **Swanson, Bret and Gilder, George. "Unleashing the 'Exaflood.'" Wall Street Journal. Feb. 22, 2008. pg. A 15.**

How the Google Cloud Works

By: Jonathan Strickland

It might not look like it, but buildings just like this one are where Google stores its clouds.
CRAIG MITCHELLDYER/GETTY IMAGES

When Larry Page and Sergey Brin began work on a project called BackRub, they probably didn't envision the enormous corporation that would grow out of their early efforts. This project evolved into Google, a juggernaut of a company that competes on a global scale with other mega corporations. While the company has products ranging from Web-based e-mail to collaborative office applications, its corporate mission has remained the same. Google intends "to organize the world's information and make it universally accessible and useful" [source: Google].

Google's search engine is the oldest and likely most famous tool in the company's arsenal. But the engineers at Google view organizing the world's information as a job too complex for just a search engine. The company designs tools and services that relate to its mission, sometimes in ways that aren't obvious at first glance. One major focus for the company is cloud computing.

Google isn't alone in offering cloud computing services. Companies like Apple and Microsoft offer products that either directly involve cloud computing services or rely on them in some way. Amazon, the online retail giant, has a thriving cloud storage business. That doesn't mean Amazon has a warehouse filled with fluffy, white clouds. It means the company rents out storage space within its massive data centers. If you are running a company that wants to offer a Web site or service to customers, you may consider using a company like Amazon to host your data.

Google also has a reputation for building enormous data centers. In The Dalles, Ore., Google has a data center built next to the Columbia River. Each building in this data center is about the size of a football field. The location has many features that make it attractive for a data center: It's near hydroelectric dams, which makes power accessible and economical. It's also in an area with a fiber-optic network, which allows for lightning-fast data transmissions [source: Markoff and Hansell].

These huge facilities are necessary for Google to carry out its corporate mission. Not only must the company search and index the world's information on the Web but it also has to provide the power for a growing network of cloud computing services. Now, let's take a look at exactly what cloud computing means.

Contents

What is Cloud Computing?

Cloud computing is a popular buzz term in technology circles. The phrase has a vague sound to it. What exactly is cloud computing?

At its most basic level, cloud computing is a model for remote computer access. The idea is simple: You use your computer and an Internet connection to make contact with a remote server. This server, which is really just a computer, runs applications using its hardware. You're able to influence the application by executing commands through a Web browser or other user interface. But the remote server is doing all the heavy lifting.

Why would you want to use a cloud computing system? One reason is that it lets you access applications your own computer might not be able to execute. Your computer only has to run a Web browser or simple user interface. In most cloud computing applications, this client-side program places minimal demands on your machine's resources. That means you can take advantage of a variety of programs and services without having to continually invest in the fastest computers. Since the cloud computing service is handling all the processor work, you just need a machine capable of connecting to the Internet.

Another major selling point for cloud computing services is that they allow you to access your data on a variety of devices no matter where you are. If you rely on your own computer to execute programs, you're limited to that machine unless you make special arrangements. You may have to e-mail a file to yourself so that you can access it on another device. You may have to set up a home network to allow file transfers between machines. And there's the risk that you'll duplicate the file in the process, which can be confusing further down the road -- which file is the real one? Cloud computing services store your information on remote servers. You can log into the cloud computing service using your account login and password. You don't have to use the same computer or device each time.

Google is in a particularly good position when it comes to cloud computing. It's a large, stable company, which means customers can be reasonably confident that their services and data won't disappear overnight. Its leadership team includes engineers who know how to create solutions for computer centers. And the company has demonstrated that its philosophy of using inexpensive equipment rather than cutting-edge machines works.

Next, we'll take a closer look at how Google creates a cloud.

Stormy Weather

Cloud computing has many advantages for the average consumer but it raises some questions. What happens if the cloud computing service goes out of business? Does your data disappear or does it get auctioned off? And who exactly owns the information stored on all those computers? If you delete your account with a cloud computing service, how sure can you be that the company will wipe your information out of the corporate database?

The Anatomy of a Cloud

Google's approach to cloud computing may seem perplexing at first. You might think a huge corporation worth billions of dollars would have data centers packed with state of the art, high-tech servers and machines that go ping. Wouldn't Google executives want the best equipment?

But Google's approach is more pragmatic. The company purchases mid-range servers for its data centers. The company has a good reason for this approach. Should something break, it's relatively

easy and inexpensive to get a replacement. Repair and maintenance can be huge costs for a data center -- each building may house thousands of machines. To ensure services remain online, Google dedicates several servers to provide the same function. That way, should one server malfunction, another can take its place with a minimal interruption in services. It builds redundancy into the system.

Google's philosophy is to keep the back end system as simple as possible. As systems become more complex, the opportunity for problems to arise increases. Simplifying a system reduces the chance for problems even if the system itself is enormous. The Google cloud's foundation is the Google File System. This is a distributed computing system that handles information requests through basic file commands like open, read and write.

The entire file system consists of networks called clusters. The Google File System relies on master servers to coordinate data requests -- each cluster has a single master server. When you interact with information stored on the cloud, your actions translate into data requests. A request may be something simple, like viewing a file, or may involve more complex actions, such as formatting or writing new data. Your computer acts as a client -- a machine that sends data requests to other machines. Ultimately, a master server takes the request and sends a message to the Google machine that houses the data -- Google calls these machines chunkservers. The chunkserver sends the data directly to the client -- the information never passes through the master server.

Because Google stores several copies of each piece of information for the sake of redundancy, making changes to data in the cloud is a little complicated. First, your write request goes to a master server. The master server chooses one chunkserver storing the appropriate data to respond to your request -- this becomes the primary replica chunkserver. The master server tells the client the location of all replica chunkservers storing your file. When you make changes, those changes go to the first replica chunkserver to which your computer can connect. The write request moves through the system to all the replica chunkservers, including the primary replica. The primary replica makes the actual change to the data and then sends a message to all other replica chunkservers to do the same. Once the primary replica receives confirmation that all copies of the data have changed, it sends a notification to the client.

Now that we have the technical details out of the way, let's take a look at some of the things you can do with the Google cloud.

Google Cloud Connect

One of the challenges of working with electronic documents is finding a simple way to collaborate with other people. Using the old method of opening up an application on your computer, creating a file, saving it and then sending it to someone else invites problems. First among those is that this approach generates two copies of the document. If you make changes to your copy while other people make changes to their copies of that same file, how do you incorporate all the changes? Which version of the file is the correct one? What happens if someone opens an older copy of the file and makes changes, not knowing that a more current version of the document already exists? File management becomes challenging.

Google Cloud Connect approaches this problem by leveraging the cloud and the application programming interface (API) for Microsoft Office. After installing a plug-in for the Microsoft Office suite of programs, you can save files to the cloud. This means the cloud copy of the file becomes the master document that everyone uses. Google Cloud Connect assigns each file a unique URL. You can

share this URL with others to let them view the document. If you designate someone as an editor, that person can then download the document and open it in Microsoft Office.

If you make changes to the document, those changes will show up for everyone else viewing it. Should other editors make changes, you'll see them reflected in your copy. When multiple people make changes to the same section of a document, Cloud Connect gives you the chance to choose which set of changes to keep.

So how does it work? When you upload a document to Google Cloud Connect, the service inserts some metadata into the file. Metadata is information about other information. In this case, the metadata identifies the file so that changes will track across all copies. The back end is similar to the Google File System and relies on the Google Docs infrastructure. As the documents sync to the master file, Google Cloud Connect sends the updated data out to all downloaded copies of the document using the metadata to guide updates to the right files.

Microsoft offers its own online collaboration tool called SharePoint. But unlike Google Cloud Connect, SharePoint isn't free. Businesses interested in SharePoint must purchase a license to use it on their computers. But since SharePoint is a Microsoft product for Microsoft Office applications, there's a tight integration of features that Google can't match.

Next, we'll look at Google's Cloud Print service.

System Requirements

To use Google Cloud Connect, you'll need a Google account and a PC running Windows XP, Vista or Windows 7. You'll also need Microsoft Office 2003, 2007 or 2010. Because the Mac version of Microsoft Office lacks an open API, there's no Google Cloud Connect solution for Apple fans yet.

Google Cloud Print

On Aug. 10, 2011, IBM executive Mark Dean caused a bit of a stir when he referred to the world being in a "post-PC era." Dean wasn't saying that the PC was dead or obsolete. But he was pointing out how people are using mobile devices more often when they perform basic activities traditionally done on computers. Smartphones and tablets are pushing desktop and laptop computers to a support role. One of those tasks is printing.

Traditionally, to send a print job to a printer you'd either have to connect the printer directly to your computer, or connect both the printer and your computer to a network. Google Cloud Print is a service that extends the printer's function to any device that can connect to the Internet. You can be on the other side of the world and send a print job to the machine sitting on your desk at home.

To use Google Cloud Print, you need the following:

- a free Google profile
- an app, program or Web site that incorporates the Google Cloud Print feature
- at least one cloud-ready printer or printer connected to a computer logged onto the Internet

When you use Google Cloud Print through an app or Web site, the print request goes through the Google servers. Google routes the request to the appropriate printer associated with your Google account. If you register more than one printer -- there's no limit to the number of printers you can connect to your account -- you'll have to designate the machine you want the print job to go to. Assuming the respective printer is on and has an active Internet connection, paper and ink, the print

job should execute on the machine even if you're in another part of the world. You can share your printer with other people, allowing them to send you printed documents through Google Cloud Print.

Because most printers aren't t cloud-ready, most Google Cloud Print users will need to have a computer act as a liaison. Google Cloud Print is an extension built into the Google Chrome. browser Google turns the setting off by default -- you have to choose to enable it. Once enabled, the service activates a small piece of code called a connector. The connector's job is to interface between the printer and the outside world. The connector uses your computer's printer software to send commands to the printer. As of this writing, Google has connectors built for PCs and Macs and is working on one for Linux machines.

If you have a cloud-ready printer, you can connect the printer to the Internet directly without the need for a dedicated computer. You have to register the cloud printer with Google Cloud Print to take advantage of its capabilities. The big advantage of the cloud printer is that you don't have to keep a computer powered on, online and connected to your Google account in order to receive print jobs. You connect a cloud printer to the Google Cloud Print service by registering the printer's unique email address with Google.

Because Google allows app and Web site developers to incorporate Google Cloud Print into their products as they see fit, there's no standard approach to executing a print job. You might see one user interface on one site and a completely different approach on another. Also, Google Cloud Print depends upon developers incorporating the feature into their products. Not every app or site will have Google Cloud Print built into it, which limits its functionality. Naturally, Google builds the service into its own products but many people rely on services from multiple sources and may find Google Cloud Print doesn't have a wide enough adoption to meet all their needs.

Keeping It Private

Sending a print job through the cloud comes with a price: privacy. When you send a print job through Google Cloud Print, you share with Google the documents themselves as they upload to the service before going to your printer. Google logs each request and so you'll leave an electronic trail with every print job. Google deletes documents once Google Cloud Print receives confirmation that a print job is complete. Google also says that no one will look at the content of your print jobs.

Google Music Cloud

Mobile access to music isn't a new trend. We've had car radios and portable radios for decades. Then came inventions like the portable cassette player, portable CD player and MP3 players. With each generation of product, we expanded our options to take our music with us on the go. But each of these gadgets gave us limited access and it wasn't always easy to share music across multiple devices. Google's Music service aims to change that.

At its most basic level, Google Music is a cloud storage service coupled with a simple music player interface. You can upload songs to your Google Music account and access them with a computer or Internet-capable device using the Google Music app. Google allows you to upload up to 20,000 songs for free. Google limits the file size for an individual song to 250 megabytes, which might require you to use a lower bit rate when converting tracks to digital files.

Google Music supports MP3 and aac files across all platforms. The Windows version of Google Music supports wma files. Linux computers support ogg files. And while you can upload FLAC files to Google

Music, Google will transcode those files into MP3 formats at 320 kbps. Because MP3 is a lossy format, this compression might have an impact on the sound quality.

While you can log into your Google Music account from multiple computers and devices, only one device can actually play music at any given time. Two people can't listen to different devices accessing the same account at the same time. This is how Google prevents people from using Google Music as a way to encourage piracy.

Even with Google's protection in place, the music industry isn't thrilled with Google Music. Google sought out deals with the record industry before launching Google Music but didn't make much progress. Eventually, the company decided to move forward with a beta test of Google Music without licenses. From Google's perspective, Google Music is like any other storage device. If you purchase a song, you're allowed to transfer that song to an MP3 player or smartphone. You could also store that song on a hard drive connected to your computer. You could even transfer it to a video game console. Google Music is like any other data storage device -- it's just that this storage device might be hundreds of miles away from the person who bought the song.

Google is still trying to make deals with record labels. Right now, the only way to get your music onto Google's service is to upload it yourself. If you have a slow connection and a large music library, this could take hours. With the proper licensing agreements, Google could incorporate a sales platform that would allow you to buy music and automatically store it to your Google Music account.

Google's cloud services are likely just the beginning of a full suite of products that will shift computing away from the consumer and onto servers. As broadband penetration spreads across the globe and the focus shifts to inexpensive computers and mobile devices, cloud services will become more compelling. Using cloud services requires a level of trust in the provider. Google will have to prove that it is reliable and ethical with its cloud services or risk alienating users. Are you willing and ready to have a company like Google handle your data and provide your computer services?

Jam Session

Google isn't the only company offering cloud-based music services. Amazon also has a cloud storage solution for music lovers. Apple has built some cloud functionality into iTunes. And then there are Internet-based music services like Spotify, Pandora and Last.fm. It's a good time to be a tech-savvy music fan!

Lots More Information

Related Articles

- **How Google Works**
- **How the Googleplex Works**
- **Why is the Google algorithm so important?**
- **How Google Plus Works**
- **How Cloud Computing Works**

More Great Links

- **Google Cloud Connect**
- **Google Cloud Print**
- **Google Music**

Sources

- **Bright, Peter. "Hands-on: Google Cloud Connect for Office not ready for prime time." Ars Technica. February 2011. (Aug. 23, 2011) http://arstechnica.com/microsoft/news/2011/03/hands-on-google-cloud-connect-for-office-not-ready-for-prime-time.ars**
- **Bruno, Antony. "Why Record Labels and Google Music Couldn't Agree on the Cloud." The Hollywood Reporter. May 12, 2011. (Aug. 24, 2011) http://www.hollywoodreporter.com/news/why-record-labels-google-music-187889**
- **Dean, Mark. "IBM Leads the Way in the Post-PC Era." A Smarter Planet Blog. Aug. 10, 2011. (Aug. 23, 2011) http://asmarterplanet.com/blog/2011/08/ibm-leads-the-way-in-the-post-pc-era.html**
- **Ghemawat, Sanjay, Gobioff, Howard and Leung, Shun-Tak. "The Google File System." Google. 2003. (Aug. 23, 2011) http://static.googleusercontent.com/external_content/untrusted_dlcp/labs.google.com/en/us/papers/gfs-sosp2003.pdf**
- **Google. "Company." Aug. 23, 2011. http://www.google.com/about/corporate/company/**
- **Google. "Google Cloud Connect." Aug. 23, 2011. http://tools.google.com/dlpage/cloudconnect**
- **Google. "Google Cloud Connect for Microsoft Office available to all." Google Docs Blog. Feb. 24, 2011. (Aug. 23, 2011) http://googledocs.blogspot.com/2011/02/google-cloud-connect-for-microsoft.html**
- **Google. "Google Cloud Print." Aug. 23, 2011. http://www.google.com/chrome/intl/en/p/cloudprint.html**
- **Google. "Google Data Centers." Aug. 24, 2011. http://www.google.com/corporate/datacenter/**
- **Google. "Google Music Beta." Aug. 24, 2011. http://music.google.com/music/listen#start_pl**
- **Google. "Music Help." Aug. 24, 2011. http://www.google.com/support/music/**
- **Harris, Robin. "Google File System Evaluation." StorageMojo. June 13, 2006. (Aug .24, 2011) http://storagemojo.com/?page_id=152**
- **Markoff, John. "Hiding in Plain Sight, Google Seeks More Power." The New York Times. June 14, 2006. (Aug. 23, 2011) http://www.nytimes.com/2006/06/14/technology/14search.html**
- **Metz, Cade. "Google Cloud Connect: The limits of a Microsoft makeover." The Register. February 2011. (Aug. 24, 2011) http://www.theregister.co.uk/2011/02/26/google_cloud_connect_caveat/**
- **Pham, Alex and Guynn, Jessica. "Google Music launches without label deals." Los Angeles Times. May 10, 2011. (Aug. 24, 2011) http://latimesblogs.latimes.com/entertainmentnewsbuzz/2011/05/google-music-launches-without-label-agreements.html**

What Is iCloud?

By: Stephanie Crawford | Updated: Mar 26, 2024

Steve Jobs introduced the iCloud service at the Apple Worldwide Developers Conference in June 2011.
JUSTIN SULLIVAN/GETTY IMAGES

Cloud storage is a growing tech trend. Making use of cloud computing technology, cloud storage services give you password-protected access to online storage space. But **what is iCloud?** It's Apple's cloud storage product.

iCloud is designed to work seamlessly with all your Apple devices connected to the Internet. For example, you can upload photos from your iPhone and access them from your MacBook, upload music from your MacBook to listen to from your iPod Touch or upload an important document from your Mac desktop to access from your iPad when you're on the go.

Contents

From MobileMe to iCloud

iCloud isn't Apple's first online storage service. MobileMe was iCloud's long-standing predecessor, offering synchronization services for an annual subscription fee. MobileMe's primary purpose was to keep certain files synchronized between multiple devices. This included e-mail, contacts, calendars, browser bookmarks, photo galleries, and Apple iWeb and iDisk services. Though MobileMe was tailor-made for Apple products, it also gave users the option to synchronize data from non-Apple computers.

Apple revamped MobileMe and merged its offerings into the iCloud service. iCloud not only replaces MobileMe, but it also adds features, flexibility, and free service for up to 5 GB of storage space. In addition, digital products you purchase through Apple's iTunes Store are available from your iCloud account without counting against that free 5 GB. Later, we'll take a closer look at iCloud's features and pricing and how they compare to other cloud storage products.

Like its MobileMe predecessor, iCloud's biggest advantage is that it's integrated into Apple software. That makes iCloud your most convenient cloud storage option if all your computers and mobile devices are Apple products. Apps you use in both macOS and Apple iOS can connect to your iCloud space and automatically store your data there, including your contacts list and photo gallery.

Now that you know what iCloud is, let's take a closer look at its features and costs, and how it keeps your data both safe and readily accessible.

Apple iCloud Service

iCloud's features give you access to your data, from important contacts to fun photos, anywhere you're connected to the Internet. You can authorize up to 10 devices to access and use iCloud with

If you upload a photo to your iCloud online storage, you'll be able to access the file from any of your Internet-connected Apple devices.
IMAGE COURTESY OF APPLE, INC.

your Apple ID. This is a leap beyond the iTunes Store authorization, which is limited to five devices. Plus, iCloud authorization extends beyond iTunes to touch all apps capable of connecting and using iCloud from that device. Developers program each app to connect to and use iCloud content in its own way, so check an app's help pages to find out whether and how it can use iCloud. If you're one of those developers, check out how your app creations can use the iCloud application programming interfaces (APIs) as described at the Apple developer site.

Besides its options for apps to connect to and use the service, iCloud features unlimited free storage for anything you purchase through the iTunes Store. This means that any music, movies, TV shows, books, or apps you purchase from iTunes don't count against your free 5 GB of iCloud storage space. In addition, each iTunes purchase is instantly available for download to any of your iCloud-authorized devices, as long as the songs are available from the iTunes store. In short, buy it once, access it everywhere. This even applies to purchases you made under the same Apple ID long before iCloud existed, provided they're still available in the iTunes Store.

It's possible that 5 GB is enough for storing your non-iTunes files in iCloud, such as documents and photos. However, Apple also realizes that you might want more space, and you can purchase subscription-based upgrades to fill that need. As of this writing, Apple is offering the following subscription options for increasing your iCloud storage space:

- 50 GB = $0.99 per month
- 200 GB = $2.99 per month
- 2 TB = $9.99 per month

Apple iCloud Advantages

Perhaps the biggest advantage of the iCloud service is how you can use it to back up and restore data on your Apple iOS devices. iCloud is capable of taking daily backups of your iPhone, iPad or iPod Touch when it's connected to the Internet using WiFi. These aren't full backups, which would include all the data stored on each device. Instead, these are partial iCloud backups that store only the data you've changed on the device. The following are the types of data that iCloud can back up from your iOS device:

- Your personal device settings, like the screen brightness or call volume
- Your app arrangement on the screen
- Ringtones and text messages
- Apps, music, and books you've purchased from iTunes
- App data, like an account setup or game scoreboard
- Photos and video associated with the Camera Roll feature in iOS

In addition to simplifying the backup process, the iCloud service makes quick work out of restoring an Apple iOS device from the iCloud backup. You'll probably want to restore your device any time you lose important data, reset or replace the device, or upgrade to new hardware.

We've looked at the features Apple iCloud has to offer. Next, let's see what challenges iCloud faces and how it stacks up to its competition in the cloud storage market.

iTunes Match

Though not a component of iCloud, another technology you can use to improve your iCloud experience is Apple's iTunes Match. This applies to music content that you've purchased from another source and added to your iTunes library. This includes, for example, music you've imported from CDs. What iTunes Match will do is identify whether that music is also available in the iTunes Store and then add that music to your iCloud library. What iTunes can't match, you can upload to iCloud. This means you'll have the same convenient access to those tracks as you have to your iTunes purchases.

iCloud's Challenges and Competition

Many of iCloud's challenges are the same as those faced by other cloud service providers. Users are limited to using software specially designed to access that particular cloud. Though iCloud is available anywhere you can access the Internet, it still requires some sort of front-end application to manage the connection between you and your data.

iCloud also faces the same Internet access challenges as other cloud player products. One way Apple has addressed this is by limiting the iCloud software so that certain interactions can only occur when using a WiFi Internet connection. This means your device won't eat up a limited 3G wireless data plan just for regularly scheduled synchronization tasks.

One unique challenge for iCloud started in a courtroom rather than a computer. Within days of Apple's June 2011 announcement naming the iCloud product, an Arizona voice-over-IP (VoIP) provider filed a lawsuit. The firm, iCloud Communications, had owned the right to its company name since 2005. Apple had filed eleven trademark applications for the iCloud name and brand and purchased a matching domain from Swedish company Xcerion. According to the U.S. Patent and Trademark Office, iCloud Communications didn't register the iCloud brand itself, leaving it up for grabs. The Arizona company dropped the lawsuit.

Since iCloud isn't the only cloud storage service out there, how does it stack up to its competition? Here's a quick look at some other cloud storage services and how they compare to iCloud:

- Amazon Cloud Drive and Cloud Player are probably the closest to iCloud in terms of how buying and using content are tied together. Both services let you upload or purchase content and access it from any device. However, because Amazon is not attached to a suite of operating system software, it doesn't have the deep OS integration that iCloud has on Mac and iOS systems. Amazon also limits your free storage space. Amazon's biggest advantage over iCloud is that it provides a music streaming option for mobile devices running Amazon MP3 Player software.
- Dropbox offers only the first 2 GB free and lacks iCloud's deep OS integration. However, it has been around a while, and enterprising developers have used its application programming interface (API) to produce well-designed Dropbox-connected apps for every major desktop and mobile operating system. Dropbox's biggest disadvantage compared to both iCloud and

Amazon is that all your stored files, no matter what type they are, count against your total storage limit.

- Google Music is designed specifically for storing and streaming music. Google Music offers features comparable to Amazon Cloud when it comes to audio tracks, but it doesn't have the flexibility of iCloud or Cloud Drive to store and synchronize all types of data.
- Microsoft Windows Live SkyDrive is designed for sharing documents, videos and photos between multiple users. In contrast, your iCloud content is limited to use by your Apple ID only. SkyDrive also offers 7 GB of storage space for free. SkyDrive is nearly as integrated with Microsoft products as iCloud is with Apple products, so choosing between them may be a matter of which type of computers and mobile devices you plan to use.

Sources

- Apple Inc. "Apple to Unveil Next Generation Software at Keynote Address on Monday, June 6." May 31, 2011. (Aug. 22, 2011) http://www.apple.com/pr/library/2011/05/31Apple-to-Unveil-Next-Generation-Software-at-Keynote-Address-on-Monday-June-6.html
- Apple Inc. "Frequently asked questions about the MobileMe transition and iCloud." (Aug. 22, 2011) http://www.apple.com/mobileme/transition.html
- Apple Inc. "iCloud Beta for Developers." (Aug. 22, 2011) http://developer.apple.com/icloud/index.php
- Apple Inc. "iCloud Features: Apps, Books, and Backup." (Aug. 22, 2011) http://www.apple.com/icloud/features/apps-books-backup.html
- Apple Inc. "iTunes Store: About authorization and deauthorization." July 15, 2011. (Aug. 23, 2011) http://support.apple.com/kb/ht1420
- Apple Inc. "MobileMe." (Aug. 22, 2011) http://www.apple.com/mobileme/
- Apple Inc. "Storage Upgrade Options." (Aug. 22, 2011) http://www.apple.com/icloud/includes/lightbox-storage.html#lightbox-storage
- Apple Inc. "What is iCloud?" (Aug. 22, 2011) http://www.apple.com/icloud/what-is.html
- Boutin, Paul. "Amazon's and Google's Cloud Services Compared." The New York Times Company. June 6, 2011. (Aug. 24, 2011) http://gadgetwise.blogs.nytimes.com/2011/06/06/amazons-and-googles-cloud-services-compared/
- Dockrill, Peter. "The calm before the cloud? Apple quietly begins music streaming." Ninemsn. Aug. 25, 2011. (Aug. 24, 2011) http://apcmag.com/the-calm-before-the-cloud-apple-quietly-begins-music-streaming.htm
- Gralla, Preston. "5 Great Microsoft Web Services You Probably Don't Use." PCWorld.com. PCWorld Communications, Inc. Mar. 3, 2009. (Aug. 24, 2011) http://www.pcworld.com/article/159413/5_great_microsoft_web_services_you_probably_dont_use.html
- Hardawar, Devindra. "Microsoft revamps SkyDrive cloud storage with HTML5, kicks Silverlight to the curb." VentureBeat. June 20, 2011. (Aug. 24, 2011)

http://venturebeat.com/2011/06/20/microsoft-revamps-skydrive-cloud-storage-with-html5-kicks-silverlight-to-the-curb/

- Hollister, Sean. "iCloud Communications sues Apple for obvious reasons." Engadget. AOL Inc. Jun. 12, 2011. (Aug. 24, 2011) http://www.engadget.com/2011/06/12/icloud-communications-sues-apple-for-obvious-reasons/
- Keizer, Gregg. "Apple likely to settle iCloud trademark lawsuit, says legal expert." Computerworld Inc. Jun. 13, 2011. (Aug. 24, 2011) http://www.computerworld.com/s/article/9217586/Apple_likely_to_settle_iCloud_trademark_lawsuit_says_legal_expert
- Milian, Mark. "Court clears cloud music providers to expand features." Cable News Network. Aug. 24, 2011. (Aug. 24, 2022) http://www.cnn.com/2011/TECH/web/08/23/cloud.music/
- Newman, Jared. "Apple iCloud: What it is, and What it Costs." PCWorld Communications, Inc. Aug. 2, 2011. (Aug. 22, 2011) http://www.pcworld.com/article/237086/apple_icloud_what_it_is_and_what_it_costs.html
- Reisinger, Don. "Apple unveils iCloud, shows off features of Lion, iOS 5." CNET. CBS Interactive. June 6, 2011. (Aug. 22, 2011) http://news.cnet.com/8301-13506_3-20069336-17/apple-unveils-icloud-shows-off-features-of-lion-ios-5/

How to Back Up Your iPhone

By: Chris Pollette

You can back up your iPhone to your computer or to the iCloud. Francesco Carta fotografo/Getty Images

Although it sometimes seems like our smartphones are always there when we need them, it's a good idea to remember they're easily lost, stolen, or broken. You can replace the hardware, but any information on your phone, including photos, recordings, documents, or saved application data will

be gone forever. Even something as simple as updating the operating system could turn your expensive smartphone into a "brick" of silicon, glass, and metal.

Fortunately, it's pretty easy to back up your iPhone, and if you get a new phone of the same type, you may be able to upload the saved files onto your new device and format it just like the old one, as long as you backed it up. iPhone users have two main options: You can save your backup to a computer, or to an iCloud account.

It's important to remember that syncing your phone is not the same as backing it up. While syncing saves contacts, photos, videos, songs, playlists, and podcasts, backing up saves a snapshot of your entire phone's contents to restore them. Here's how to back up your phone to your computer:

1. Plug your phone into your Mac. If your computer is running MacOS 10.14 Mojave or an older system, you'll need to open iTunes to access your phone. If your computer has MacOS 10.15 or newer, you can locate your phone via the Finder (at the bottom of your screen).
2. If a message asks for your device passcode or to Trust This Computer on your phone or computer, follow the onscreen steps. (Apple has support resources if you've forgotten your passcode.)
3. Locate your device on the computer (if it doesn't appear automatically, use these instructions to find it).
4. If you have sensitive information of any kind, especially financial or health information, it's a very good idea to encrypt your backup for security. (If you don't want to encrypt your information, skip this step.)
5. Even if you don't elect to encrypt your backup, the phone will update your apps and the OS before doing the transfer of your contents.
6. Click Back Up Now and wait for the contents to transfer.

Windows users must use Apple's iTunes software to back up their iPhones. Click on your iPhone in the iTunes window, and click Summary. Then click on Back Up Now, and you'll have the option to encrypt your backup.

You can also back up your iPhone wirelessly using an iCloud account. Here's how:

1. Connect your device to a WiFi network.
2. In System Preferences, tap the option with your name at the top of the screen.
3. Click iCloud, then iCloud Backup.
4. Click Back Up Now.

It's important to remember that the amount of storage you have on your iCloud account may limit how much you can back up. Simply put if you have the free 5 GB account and a 256 GB iPhone, you will need to pay for more storage or back up to your computer instead. Unlike computer backups, all iPhone backups to iCloud are fully encrypted for security.

There are also third-party software solutions to help with Windows and Mac backups, such as Acronis True Image, iMazing, and Dr.Fone. Third-party software may offer additional backup options, including the ability to choose the location of your backups and select the parts of the backup to restore.

How to Back Up Your Android Phone

To back up your Android phone, utilize Google Drive's built-in backup feature. Open your phone's Settings, navigate to "Google," then "Backup," and enable "Back up to Google Drive." This will automatically back up your device's data to your Google account, including contacts, app data, and more.

Detailed Steps:

1. **Open Settings:**

Launch the Settings app on your Android phone.

2. **Navigate to Google:**

Tap on "Google" or "Accounts and backup," depending on your device's interface.

3. **Access Backup:**

Within the Google settings, find and tap on "Backup" or "Backup and restore," according to Google Help.

4. **Enable Backup:**

If prompted, follow the on-screen instructions to turn on "Back up to Google Drive" or "Backup by Google One".

5. **Configure Settings (Optional):**

You can customize your backup settings, such as choosing specific data to back up or setting up automatic backups while the phone is charging and connected to Wi-Fi, says Google One Help.

6. **Initiate Backup:**

Tap "Back up now" to start the backup process or to ensure that it's enabled for automatic backups.

7. **Review Backup Details:**

You can review your backup settings and manage your backups through the Google One app or by navigating back to the Backup settings in your phone's settings.

Additional Notes:

- **Samsung Cloud:** If you have a Samsung phone, you can also back up to Samsung Cloud.
- **Third-party apps:** Numerous third-party apps provide comprehensive backup solutions for Android phones.
- **Manual backups:** You can also manually back up specific files and folders by connecting your phone to a computer via USB and copying the desired files.

Back up or restore data on your Android device

You can back up content, data and settings from your phone to your Google Account. You can restore your backed up information to the original phone or to some other Android phones. You can't use back up when you set up a personal device with a work profile or for work only, or when you set up a company-owned device.

Restoring data varies by phone and Android version. You can't restore a backup from a higher Android version onto a phone running a lower Android version.

Important: Some of these steps work only on Android 9 and up. Learn how to check your Android version.

Where your phone data is stored

Your backups are uploaded to Google. Some of your data is end-to-end encrypted with your device's screen lock PIN, pattern or password.

How your data is protected

Your data is encrypted to help keep it safe and secure.

- All data, including photos and videos, messages and more, are encrypted as they move between your device, Google services and our data centres.
- Some data is further encrypted with your device's screen lock. Photos and videos in Google Photos and MMS media received from your operator aren't encrypted by your device's screen lock.

Tip: To hide sensitive photos and videos with your screen lock, you can save them to a special folder in the Google Photos app. Learn how to hide your sensitive photos and videos.

Automatically back up your device

Important: To help protect your backed-up data, use a PIN, pattern or password screen lock instead of a swipe or Smart Lock.

You can set up your device to automatically back up your files.

1. Open your device's Settings app.
2. Tap **Google** > **All services**.
3. Under 'Backup and restore', tap **Backup**.
   Tips:
   - If this is your first time, turn on **Back up your device with Google One** and follow the on-screen instructions.
   - Select the data that you want to back up: **Photos and videos**, **Device data** or both.
4. Turn **Backup by Google One** on or off.

Your Google One backup can take up to 24 hours. When your data is saved, 'On' will be displayed below the data types that you selected.

Add or switch backup accounts

What gets backed up

Manually back up data and settings

1. On your Android device, open your device's Settings app.
2. Tap **Google** > **All services**.

3. Under 'Backup and restore', tap **Backup** › **Back up now**.

Erase after backing up

After you back up, you can reset your device by erasing everything on it. Learn how to reset your device to factory settings.

Get your data onto a new device

When you add your Google Account to a phone that's been set up, what you'd previously backed up for that Google Account gets put onto the phone.

To restore a backed-up account to a reset phone, follow the on-screen steps. For more help, get help from your device manufacturer.

Your photos and videos are already available in Google Photos. But you can restore the rest of the data that you backed up while you set up your new phone for the first time or after a factory reset. At setup, to restore your data, follow the on-screen steps.

The process can take up to 24 hours.

Important: Both devices must be on the same Android version or your new device must be on a later Android version. If your new device is on an older Android version than your previous device, it may result in an incomplete data transfer. Find out how to check and update your Android version.

Check which photos, data and settings you backed up

Restore backed-up contacts

How backup handles your data

Important: The data that backup collects is encrypted in transit.

Backup sends your data to Google's backup servers and helps you to transfer data between devices. Backup collects certain information to perform services on your device. Some of this functionality uses Google Play services. For example, backup collects:

- Messages, contacts, app settings and preferences are collected as part of your personal backup.
- Personal identifiers are collected to ensure that your backups are associated with you and your account.
- Crash logs and diagnostics are collected for analytics and troubleshooting purposes.

Turn backup off

To disable your backup:

1. Tap **Settings** › **Google** › **All services**.
2. Under 'Backup and restore', tap **Backup**.
3. Turn off **Backup by Google One**.

Related resources

- Back up photos and videos

- Save files and folders to Google Drive
- Back up and restore contacts from a phone or SIM card
- Recover a recently deleted Google Account
- Transfer files between your computer and phone
- Transfer WhatsApp data to a new Android

How to Back Up a Hard Drive

By: Josh Briggs

The Altair 8800 didn't have a hard drive to back up.
AP PHOTO/HEINZ NIXDORF MUSEUMSFORUM

Personal computers are perhaps the most significant invention of the 20th century. Nearly every industry relies on them. Even trades such as construction and deep sea fishing utilize computers to improve efficiency. But personal computers can also be frustrating. If you use one long enough, you'll probably encounter some sort of malfunction or hiccup that causes you to either lose productivity or worse, all your work.

Personal computers weren't always complex. The Altair 8800 was a basic 8-bit computer released in 1975 that did very little in the way of computing. Hobbyists bought them and tinkered with them -- even though there were no monitors. Running programs allowed Altair users to watch LEDs flicker in sequence. The Altair had no hard drive.

Fast-forward 30 years, and computers have become as vital to our society as the automobile. We store our lives on our computers. Bank account information, pictures from family gatherings and personal information that we consider vital to our very existence is stored in computers. As far as computers have come, the advent of the Internet has changed the game. But as useful as the Internet undoubtedly is, it comes with its fair share of baggage, including viruses and other malicious programs.

Whether you fall prey to one of the people whose hobby is to turn your computer into a boat anchor or your machine is nearing the end of its natural life, it's imperative you back up the data on your hard drive. This article will give you the tools you need to protect yourself from losing all your important data stored on your computer.

Let's start by taking a look on the next page at what you can do to minimize the damage by being proactive with your data storage.

Contents

Hard Drive Backup Solutions

To make backing up your hard drive as easy as possible, you should set up a backup profile. Most PCs with Microsoft Windows XP have a program called Windows XP Back Up installed as a useful application. Once you open the application, you can follow the instructions from the backup wizard and decide what exactly you wish to back up. If your computer's hard drive is split into separate drives or partitioned, you can chose to copy back to the original drive. This should safely store your data and be retrievable should your hard drive crash -- though if you have corrupted data, this option may not be as helpful.

Macintosh computers with Mac OS 10.5 or later have a similar application called Time Machine. This application allows you to back up data and set up a profile that will allow you to save it on the machine or export it to an external hard drive. We'll get to those in the next section.

Both of these applications give you the option of setting up a schedule to perform backups. This allows you to back up data regularly should you forget. What's more, these applications can send you e-mail alerts when performing backups if the system experiences a malfunction. You don't have to use either of these programs, however; there are lots of off-the-shelf backup solutions available for both Windows and Mac, though they come at an additional cost, of course.

Once you've mastered how to back up data on your computer, you've taken a big step toward protecting your important information. Now let's look into some external places you can store that important data to be able to retrieve it even if you do lose your primary hard drive. In the next section, we'll explore some devices and methods you can use in your defence against the unknown mysteries of hard drive failures.

Fear Factor Y2K

At the turn of the 21st century, the word on the street was that computers around the world were going to crash at the stroke of midnight, Jan. 1, 2000. The world spent an estimated $500 billion to make what people thought were necessary changes to computer software systems. Some people thought the world would end. Others thought the United States and Russia would enter into some sort of doomsday movie scenario and launch nuclear missiles at each other. In the end, nothing of the sort happened. The Y2K bug, as it was dubbed, affected very little. It may have been nothing to worry about, or perhaps all that preparation paid off. One thing to note, however; upgrades to New York City's infrastructure may have helped the city's systems' ability to withstand the attacks on Sept. 11, 2001.

External Hard Drive Backup Options

External hard drives are very convenient backup solutions, but they can be damaged and stolen.
© ISTOCKPHOTO/PIXELAXEL

Now that you've learned some reasons why to back up your data, let's explore the places you can send your data in order to retrieve it safely should you encounter some sort of computer meltdown.

One option is to export your data to an external hard drive. These devices are readily available at your local retail store and can be found at various Web sites online. Most of these drives connect to your desktop or laptop computer through the universal serial bus (USB) port on your machine. Installation is usually a matter of plugging them in and letting your operating system discover them. Many of them come with third-party software to help you back them up. One installed, you can access your external hard drive much the same way you would access your internal drive or another device connected to the computer. Backing up your data is as simple as clicking and dragging those files you wish to back up into the external drive. This is perhaps the best solution for backing up your hard drive. Your data is safe on the external hard drive should your computer crash.

A second option, one which is gathering more popularity, is **cloud storage**, backing data up online to a virtual location. There are lots of cloud storage sites on the Web; many offer a few gigabytes of storage for free but require you to pay for more space. Many of these sites boast security measures aimed to protect your vital information such as Social Security, bank and credit account numbers. Still, anytime you put information on the Web, you should do so with caution. Information on the Web, no matter how secure, is susceptible to hackers and security breaches.

If you want, you can back up your hard drive on CDs, DVDs or on a flash drive. CDs have a relatively small amount of storage space and are better for smaller data backups. DVDs can handle about seven times more information than CDs. Most CDs and DVDs are designed to be used once and can't be rewritten, though you can buy discs that can be erased and reburned when you back up your computer again. Flash drives, in comparison, can handle a few gigabytes of information and can be rewritten the same way you would with a regular hard drive. The downside is that larger flash drives can be costly, which makes backing up an entire hard drive an expensive proposition. If you use removable media, you can lock your backups in a fire safe or safety deposit box -- which you can't do with cloud storage and you may be less likely to do with an external hard drive.

If your hard drive crashes, chances are good that you will lose some data. But taking a proactive stance by backing up your hard drive will limit the damage. It's better to lose a few files than a whole life's worth of work and information. For more on hard drives, viruses and related articles, take a look at the links on the next page.

Lots More Information

Related How Stuff Works Articles

- How Hard Disks Work
- How to Add a Hard Drive to Your Computer in 8 Steps
- How To Fix Your Zombie Computer
- Computer Security Quiz
- How Computer Viruses Work
- How Firewalls Work
- How Web Servers Work
- How Hackers Work
- How Zombie Computers Work
- 10 Worst Computer Viruses of All Time
- How to Detect Online Scams

Sources

- Barlow, Gene. User Group Relations. "Perfect Backup Approach." August, 2004. (March 24, 2009) http://www.ugr.com/nl0804.html
- BBC News. "Was Y2K Bug a Boost?" Jan. 4, 2000. (March 27, 2009) http://news.bbc.co.uk/1/hi/sci/tech/590932.stm

- Microsoft. "Windows XP Backup Made Easy." (March, 25 2009) http://www.microsoft.com/windowsxp/using/setup/learnmore/bott_03july14.mspx
- Mims, Forest M. III. Creative Computing. "The Altair Story; Early Days at MITS." November, 1984. (March, 27, 2009) http://www.atarimagazines.com/creative/v10n11/17_The_Altair_story_early_d.php
- Slavin, Lois. MIT News. "Y2K Readiness Helped New York after 9/11." Nov. 20, 2002. (March 25, 2009) http://web.mit.edu/newsoffice/2002/terror-1120.html

How to Wipe a Computer: 10 Things to Do

By: Patrick J. Kiger | Updated: Mar 7, 2024

Before you sell or donate your used computer, how do you ensure the hard drive data is cleared?
ISTOCK/THINKSTOCK

When you're upgrading to a new computer, you might find yourself unsure what to do with your old one. Sure, you could sell it on eBay or Facebook Marketplace. But you need to know **how to wipe a computer**, so you can ensure that the sensitive data on your PC — financial records, passwords to credit card websites, important e-mails, and drunken pics from spring break — doesn't fall into the wrong hands.

While this can be intimidating, don't panic. In this article, we'll show you how to wipe a computer of personal information. With these vital tips, you'll be able to sell or donate your computer at factory default settings, giving you total peace of mind.

Contents

11: Personal Files Can Be Costly

Data thieves can use various programs to recover your sensitive files, even if you think you've deleted them. Just ask a British man who had to pay 100 pounds to a crook in Latvia to get back his old hard drive, after the crook mailed him a picture showing how he'd recovered his bank statements and a

mortgage application. The man had been told earlier by a computer company that his faulty hard drive would be scrubbed when it was replaced [source: Arthur].

And this is not an isolated case. In 2009, British security researchers purchased 300 used computers from several countries and then perused the hard drives. They found that one-third of them still contained data from the former owners, including medical records from hospitals, proprietary business documents, and even test-launch information for ground-to-air missiles [source: Lamb].

10: Resell or Recycle?

Don't throw out that old computer. It has a lot of materials that are hazardous in a landfill.
ISTOCK/THINKSTOCK

The first question is what to do with your old computer? If your PC or Mac is more than ten years old and unable to run the latest software, the answer is probably to recycle it.

Whatever you do, don't throw your computer away. It contains a lot of materials that are hazardous in a regular landfill, including heavy metals such as mercury, cadmium and lead [source: Tsydenova and Begtsson]. Also, many of the materials in computer parts can be extracted and reused to make new products, reducing the need to mine new materials. All you need to do is remove your computer's hard drive and take the other pieces to a local electronics recycling center.

If you have a newer computer, it would be better to sell or donate it. Decide whether to wipe the drive yourself or hire a professional to do the job. You can take your PC to one of Microsoft's certified refurbishers, who'll wipe it using state-of-the-art security methods.

For Mac computers, they can be shipped to Apple and you'll get credit at the Apple store if the company determines the computer has some monetary value [source: Apple]. However, if you're a reasonably tech-savvy person, read on to learn how to clean it yourself.

9: Back Up Data Onto a Portable Drive

Backing up your data on a portable drive will give you an extra copy for emergencies as well as allow you to transfer your data to your new computer.
ISTOCK/THINKSTOCK

If you have a PC, before you do anything else, copy all the stuff you want to keep onto a portable drive and then recopy it onto the hard disk drive of your new computer. That way, you have an extra copy of your important data in case something goes wrong. You can also use a Microsoft utility called Windows Easy Transfer that lets you choose what you want to move over to your new machine, including documents, music, pictures, e-mail, system preferences, and user accounts. Use this utility along with a special cable to hook up your old and new PCs and transfer the data directly between them [sources: Microsoft].

Another option is to transfer files from your old PC onto a portable drive by attaching the drive to a USB port. You open both your hard drive and the portable drive in separate Windows Explorer windows and then click and drag your files and directories onto the portable drive. One advantage is that it also lets you do a little housekeeping and ditch stuff that you don't need anymore.

If you have a Mac, you don't need the portable drive, because you can transfer files directly from one machine to another using a FireWire or ThunderBolt cable connection. Use a program called Migration Assistant found in Applications/Utilities. Finally, data on both PCs and Macs can be transferred wirelessly if they are both on the same network.

8: Deactivate/Deauthorize Your Software

To transfer your iTunes data, you have to deauthorize the program from your old computer and authorize it on your new one.
APPLE

Back in the day — we're talking about the late 1980s and early 1990s — you could easily copy your old software programs (or somebody else's, if you didn't have strong feelings about software piracy) and reinstall them on your new PC. These days, however, software manufacturers are pretty strict about making sure that you've paid for every program that you use. That means you have to deactivate your programs and then transfer the licenses to your new computer.

Go through your old computer's software and make a list of the programs that you'll keep, and figure out the process for deactivating and transferring the programs. That can vary from manufacturer to manufacturer [source: Owen].

For Adobe Photoshop, for example, go to Creative Cloud, the company's online platform, and sign out of the program on your old PC. Then, install the software on your new machine and sign in [source: Adobe]. With iTunes, you actually have to deauthorize the copy of the software on your old machine, then sign in and authorize the program on your new machine before you can transfer your settings and iTunes purchases from Apple's cloud.

7: Destroy Your Drive or Reuse It?

Make sure you replace your old hard drive with the same model.
ISTOCK/THINKSTOCK

As we mentioned, it's possible to dismantle a PC, take out the hard drive, and recycle the rest of the parts. But if you feel guilty about wasting the still-functional motherboard, memory chips, and intel processor in your old machine, you can pull out the old hard drive with your data and replace it with a blank refurbished hard drive on the cheap [source: Newegg].

Installing a new hard drive really isn't much more difficult than plugging and unplugging cables and turning a few screws. The key aspect of this setup process is to replace the old drive with one that's the same type.

6: Determine the Best Way to Destroy Your Drive

Smashing your hard drive with a hammer will definitely destroy the data but there are more elaborate ways too.
ISTOCK/THINKSTOCK

There are differing opinions about how to best destroy computer hardware. Some suggest simply yanking out your hard drive, slipping on a pair of goggles for safety, and then smashing it several times with a hammer [source: Lamb].

Others recommend more elaborate measures — drilling holes or pounding nails through the drive; throwing it in a fire; cooking it in a microwave oven; or soaking it in diluted hydrochloric or muriatic acid. That all sounds a bit fiendish and can be hazardous to your health as well (acid baths give off toxic fumes).

A comparatively safer method involves disassembling the drive, removing the platters, and then sanding or grinding their surfaces to make them unreadable. You may have to invest $20 or so in a special set of screwdriver bits to remove the small screws that hold the drive's case in place, though you could also try a large flat-head screwdriver to pry it off [source: O'Reilly].

If you're a fan of the TV series "Breaking Bad," you may have seen the episode in which the characters park a powerful magnet next to a police evidence room to destroy incriminating data on a drive. In real life, that process, called degaussing, probably wouldn't work unless you had a really, really powerful magnet and focused its field very precisely [source: Lynn].

5: Have a Copy of the Operating System to Reinstall

If you don't have your backup copy of your Windows operating system, you can get one from the Microsoft website.
MICROSOFT

Whether you're going to tear out your old drive and replace it, or wipe and reuse your old one, no computer will run without an operating system. If you have a Windows computer of a certain vintage, it probably came with a backup disk that you can use to reinstall the operating system after you've done your cleanup.

If not, third party tools can help you out. You can snag another copy from Microsoft via the Digital River website, and install it on a USB drive with at least 4 gigabytes of space, using the Windows 7/USB/DVD download tool. To activate the software, you'll need the Windows 7 product key, which should be on a sticker on your computer case.

If you've got a really old Mac, you'll need a disk with the operating system installation files as well. But if you've got a recent release such as Lion or Mountain Lion, you don't need one. Instead, after you erase the data on your drive, you can run a utility that will download the OS from Apple and reinstall it. We'll give you more detailed instructions later [source: Arndt].

4: Erase Your Data from the Hard Drive

In addition to deleting your files, you should use a software program designed to wipe your hard drive clean.
ISTOCK/THINKSTOCK

Unfortunately, holding down the power button isn't enough for this job! Besides, you can't just rely upon deleting your files, because security experts say that stuff can be recovered by a sophisticated data thief. In fact, traces of data may remain, even if your repartition and reformat the drive.

That's why you should use one of the numerous software programs designed to obliterate your information, such as DBAN or Lavasoft File Shredder. The latter has the advantage of allowing you to wipe out sensitive data but leave other stuff that doesn't put you at risk [source: Lamb].

With a Mac, this process is easier. Just boot up your computer from the recovery partition by holding down the command and R keys as it restarts. Then open Disk Utility. Once in your disk utility sidebar and under the Erase tab's security options, choose 7-Pass Erase, which will overwrite your data seven times, obliterating it. This is going to take several hours, so bring along your tablet and read an e-book [source: Arndt].

3: Reformat the Hard Drive

Once you reformat your hard drive, all traces of old data are gone.
ISTOCK/THINKSTOCK

This is the step that's a little scary, because of its finality. Once you reformat a drive, you wipe clean the remaining traces of data, the software programs, and the operating system. On the other hand, that isn't necessarily a bad thing, because you're also going to undo any software problems and destroy any malware that's infected the PC. So eventually, once you reinstall a new copy of the operating system, it may run even better than before [source: Phelps].

The first step is to repartition your hard drive. If you have a Windows PC, you can do this by opening the Windows Control Panel and clicking System and Security, followed by Administrative Tools, and double-clicking on Computer Management. You'll probably have to provide the password for your main user account, the one with administrator privileges that allows you to alter the computer's settings.

Once you select Disk Utility, go to the Storage menu, and click Disk Management and then New Simple Volume. That will bring up a wizard program that will guide you through the rest of the process [source: Microsoft]. The process could take a few hours to complete.

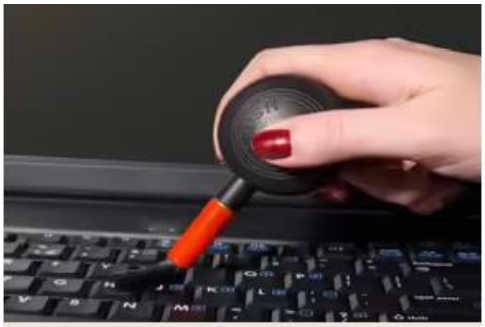
2: Reinstall the Operating System

Use your Windows disk to reinstall the operating system on your PC; for a Mac, you can reinstall through Apple's cloud. MICROSOFT

Normally, if you need to reinstall Windows because of a computer malfunction, you simply go to the Advanced Recovery Methods menu in Control Panel and then reconstruct the operating system from a recovery image that your manufacturer has installed in a separate partition on your drive. But remember that you've easily wiped all of that out. So you're going to need to use an installation disk. If you don't have the one that the computer came with, go to Microsoft for a copy and follow the onscreen instructions.

With a Mac running OS Lion or Mountain Lion, this is even easier. After you've completed erasing your data, quit Disk Utility, and make sure that you're still connected to the Internet. Then, in the Apple menu, choose the Reinstall OS X option, and Apple's cloud will do the rest. If you're running an earlier version of OS X, you'll need to put a backup system disk in the drive and click restart while holding down the C key [source: Arndt].

1: Make the Computer Shine



You can use a special brush to get the dirt out of the keyboard or just give it a gentle shake and dust with a cloth. HEMERA/THINKSTOCK

OK, by this point, your old computer is at factory settings and you've taken care to ensure the security of your personal files. But while it might be clean on the inside, the next owner, assuming you have one lined up, isn't going to like getting a machine that's covered with fingerprints and pizza remnants.

So be considerate and give your old machine a good external cleaning, using a soft damp cloth and compressed air to get particles out from the crevices in your keyboard. If it's a desktop, you can also unscrew the door on the case and use the compressed air to clean out dust bunnies on the inside. For a laptop, carefully turn the machine upside down and gently shake out the crumbs and dust in the keyboard.

Finally, use a soft glasses cloth to wipe away smears and fingerprints from the screen. You'll feel better that you did [source: Asch].

Wipe Computer FAQ

How do you wipe a computer clean to sell it?

The first thing you need to do to wipe a computer is to backup all your data onto an external hard drive. To wipe your computer clean your first option is to take out the hard drive and either destroy it or reuse it. Another option is to use a software program to erase your data from the hard drive. Alternately, you can reformat your hard drive.

Is it okay to factory reset a laptop?

It is a good idea to factory reset your laptop, especially if it is having problems with the operating system. Factory resets allow you to fix large application errors or other OS issues. They also wipe out most malware and other unwanted programs that may have found their way into the system.

Is it possible to completely wipe a computer?

It is possible to completely wipe a computer. However, security experts say that sometimes data is still recoverable by a sophisticated hacker. Even if you repartition and reformat the drive, traces of data might be left behind.

Is it a good idea to wipe your computer?

It is a good idea to wipe your computer if you are planning to upgrade to a new system, or are selling or recycling an old computer. Wiping the computer not only gets rid of any malware, but also ensures that the sensitive data and personal information stored on your PC doesn't fall into the wrong hands.

What does it mean to wipe your computer?

Wiping your computer refers to making all data on a hard drive unreadable. Wiping is often used to remove data stored on a computer inaccessible before disposing of the device.

Lots More Information

Related Articles

- Quiz: Is Your Computer Secure?
- How to Back Up Your Hard Drive
- How to Recover Lost Data

Sources

- Adobe. "Activation, deactivation | Sign in, sign out | Adobe products." (Oct. 21, 2013) http://helpx.adobe.com/x-productkb/policy-pricing/activation-deactivation-products.html
- Apple. "iTunes store: About authorization and deauthorization." (Oct. 21, 2013) http://support.apple.com/kb/HT1420
- Apple. "How to use Migration Assistant to transfer files from another Mac." (Oct. 21, 2013) http://support.apple.com/kb/HT4889
- Apple. "Reuse and Recycling Program." (Oct. 20, 2013) http://www.apple.com/recycling/gift-card/
- Arndt, Rachel Z. "How to Wipe Your Computer Before You Sell It." Popular Mechanics. Aug. 7, 2013. (Oct. 20, 2013) http://www.popularmechanics.com/technology/how-to/tips/how-to-wipe-your-computer-before-you-sell-it-15780981
- Arthur, Charles. "Before you sell your computer, smash the hard drive, says Which?" The Guardian. Jan. 8, 2009. (Oct.21, 2013) http://www.theguardian.com/technology/2009/jan/08/hard-drive-security-which
- Asch, Josh. "How to Prepare a Used Mac for Sale." Gigaom.com. Feb. 25, 2011. (Oct. 20, 2013) http://gigaom.com/2011/02/25/how-to-prepare-a-used-mac-for-sale/
- E-cycle St. Louis. "Why Recycle Electronics?" (Oct. 20, 2013) http://www.ecyclestlouis.org/why.php

- Intel. "How to Transfer Files from PC to PC." (Oct. 21, 2013) http://www.intel.com/content/www/us/en/tech-tips-and-tricks/how-to-transfer-files-to-a-new-computer.html
- Kelleher, Andrew. "Responsible Hard-Drive Destruction - Let's Get Real." Semshred.com. December 2010. (Oct. 6, 2013) http://www.semshred.com/contentmgr/showdetails.php/id/2480
- Lamb, Gregory M. "Read this before you sell or recycle your computer!" Christian Science Monitor. June 11, 2009. (Oct. 6, 2013) http://www.csmonitor.com/Innovation/Responsible-Tech/2009/0611/read-this-before-you-sell-or-recycle-your-computer
- Lynn, Samara. "Can a Magnet Zap a Hard Drive as Depicted on Breaking Bad?" PCmag.com. July 16, 2012. (Oct. 20, 2013)http://www.pcmag.com/article2/0,2817,2407192,00.asp
- Microsoft. "Create and Format a Hard Disk Partition." (Oct. 21, 2013) http://windows.microsoft.com/en-us/windows/create-format-hard-disk-partition#create-format-hard-disk-partition=windows-7
- Microsoft. "How does Windows Easy Transfer make setting up a computer easier?" (Oct. 21, 2013) http://windows.microsoft.com/en-us/windows7/how-does-windows-easy-transfer-make-setting-up-a-computer-easier
- Microsoft. "How to more safely dispose of computers and other devices." (Oct. 21, 2013) http://www.microsoft.com/security/online-privacy/safely-dispose-computers-and-devices.aspx
- Microsoft. "Installing and Reinstalling Windows 7." (Oct. 21, 2013) http://windows.microsoft.com/en-us/windows7/installing-and-reinstalling-windows-7
- Newegg.com. "Seagate ST3120215ACE 120GB 7200 RPM 2MB Cache IDE Ultra ATA100 / ATA-6 3.5" Internal Hard Drive Bare Drive." Newegg.com. (Oct. 21, 2013) http://www.newegg.com/Product/Product.aspx?Item=N82E16822148691
- O'Reilly, Dennis. "The right way to destroy an old hard drive." Cnet.com. March 26, 2009. http://news.cnet.com/8301-13880_3-10204724-68.html
- Owen, Dave. "Software Migration - Moving to a new computer." Media College. (Oct. 21, 2013) http://www.mediacollege.com/software/migration/
- Siegle, Lucy. What is the Lifespan of a Laptop?" The Guardian. Jan. 12, 2013. (Oct. 20, 2013) http://www.theguardian.com/environment/2013/jan/13/lifespan-laptop-pc-planned-obsolescence
- Smith, Matt. "How To Install A New Hard Drive To Replace An Old One." Makeuseof.com. Jan. 25, 2011. (Oct. 21, 2013) http://www.makeuseof.com/tag/install-hard-drive-replace/
- Tsydenova, O. and Bengtsson, M. "Chemical hazards associated with treatment of waste electrical and electronic equipment." Waste Management. January 2011. (Oct. 21, 2013) http://www.ncbi.nlm.nih.gov/pubmed/20869229

How to Wipe a Computer's Hard Drive

By: Talon Homer

Wiping your computer's hard drive doesn't have to involve destroying it with a hammer. You can follow a few simple steps to erase your files and start with a clean slate. Peter Dazeley/Getty Images

When electronics meet their useful end, selling or donating them is a responsible choice. It allows someone down the line to get extra use of a finely aged device, keeps the thing out of a landfill, and it may also make you a little bit of money.

However, you need to take precautions when passing along personal computers. They contain personal information like bank statements, family photos and work documents. This data should be backed up for your safekeeping, then wiped clean from the old devices. In this guide, we will show you the complete process of **how to wipe a hard drive** on both Windows and Mac machines.

For technical reasons, simply clicking "delete" on a file or dragging it to the trash bin isn't going to cut it. This is because data on a hard drive isn't actually deleted by this command. The PC's operating system simply hides it from view, which is why files can easily be taken back out of the trash.

When the bin is emptied that digital real-estate on the hard drive or solid-state drive (SSD) will be marked as open, but the actual data will remain until another file comes along to overwrite it. For this reason, data recovery services can be used to rescue files that are accidentally deleted or corrupted, but they can also be used to obtain someone else's sensitive info. SSDs in particular are very susceptible to data recovery methods.

To prevent files from being recovered off your old computer, the drive must be wiped at the system level, and that requires some digging through settings. This wiping process not only deletes all files in the typical method, but also painstakingly overwrites every bit of data in the drive to make file recovery near-impossible. Since this deletion is permanent, the first thing you'll want to do is transfer anything worth keeping over to an external drive. Once that's taken care of, the actual wiping can begin.

This process varies depending on the computer's operating system, so we've listed the steps required for Windows 8, 10 and 11, and recent versions of MacOS. Completely erasing the device can take up to a few hours, so be sure to keep the device plugged in until the process is complete.

Contents

System Wipe, Windows 8.1 or 10

If you're using Windows 8.1 or 10, wiping your hard drive is easy. Just follow these steps:

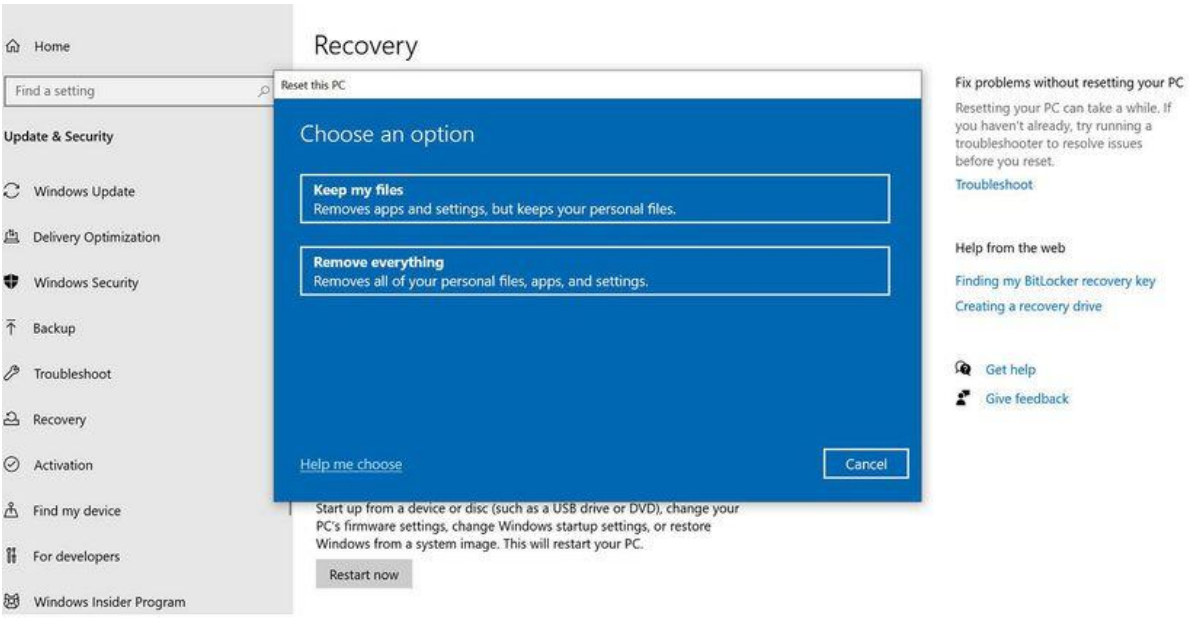
1. Select Settings (the gear icon on the Start menu)
2. Select Update & Security, then Recovery
3. Choose Remove Everything, then Remove files and Clean the drive
4. Then click Next, Reset and Continue

You may be asked whether you would like to remove files "quickly" or "thoroughly." Select thoroughly to ensure that data cannot be recovered.

System Wipe, Windows 11

To reset a PC using Windows 11, follows these steps from Microsoft support:

1. Select Start > Settings > System > Recovery
2. Open Recovery settings
3. Next to Reset this PC, select Reset PC. Open the dropdown table
4. Select Remove Everything
5. Data erasure will be set to "on" by default. Leave it at that setting for a full system wipe.



Wiping a hard drive on a PC is pretty simple. But be sure you have backed up all the files you need before you hit the OK button.

HowStuffWorks

System Wipe, MacOS

When performing a system wipe on Mac computers, there are a few extra things to be aware of. The steps can change based on which processor your Mac has, and potentially which update of MacOS it has.

There is one method for older Intel processors, and another for the proprietary Silicon chips that have been released in the past couple of years. Additionally, there is a third method that came about with MacOS' latest update, Monterey, in October 2021. All Silicon-based Macs support the Monterey update, but some of the Intel-based do not.

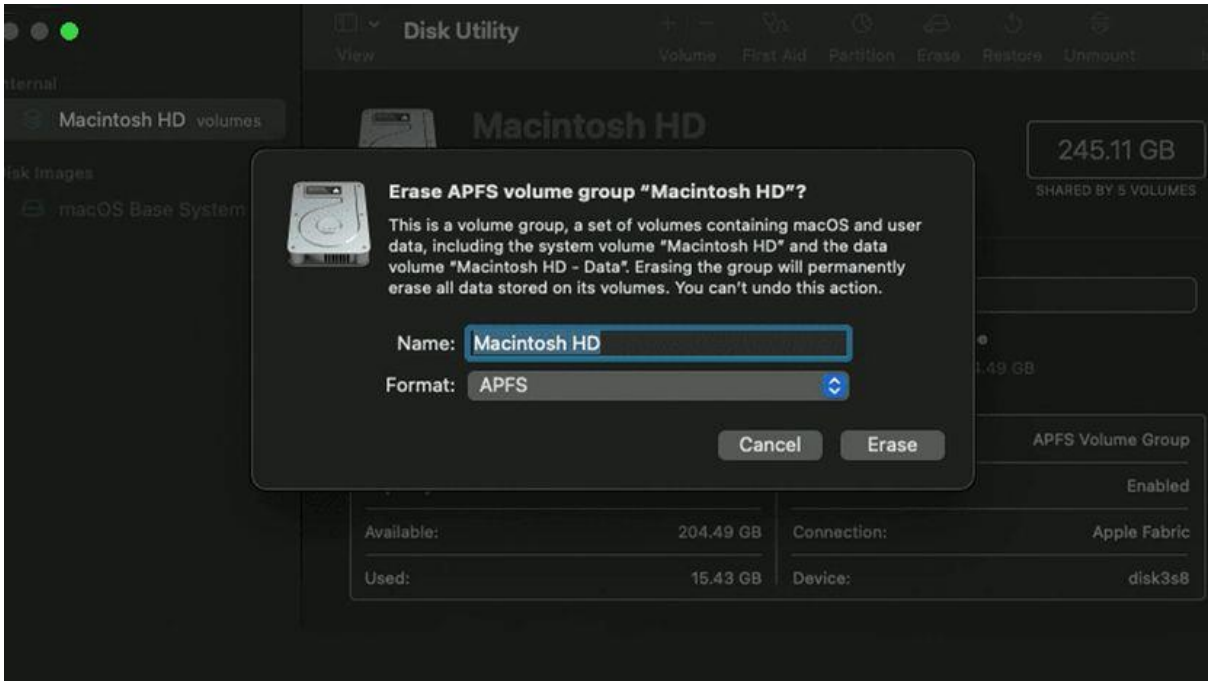
If you're unsure which processor and OS the computer has, you can find these specs by clicking the Apple menu in the top left corner of the screen, then selecting "About This Mac" in the dropdown. If your computer is running a previous version of MacOS, such as Big Sur, then your method of wiping will be determined by the brand of CPU.

System Wipe, Intel CPU

If your Intel-based Mac is running a version of the OS pre-October 2021, follow these steps from Apple:

1. Start up from macOS Recovery: Turn on your Mac, then immediately press and hold Command (⌘) and R until you see an Apple logo.
2. If asked, select a user you know the password for, then enter their administrator password.
3. From the utilities window, select Disk Utility and click Continue.
4. Select Macintosh HD in the sidebar of Disk Utility.

5. Click the Erase button in the toolbar, then enter the requested details: Name: Macintosh HD Format: APFS or macOS Extended (Journaled), as recommended by Disk Utility
6. Click Erase. However, if you see an Erase Volume Group button, click that button instead
7. If asked, enter your Apple ID.
8. After the erase is complete, select any other internal volumes in the sidebar, then click the delete volume (–) button in the toolbar to delete that volume.
9. Quit Disk Utility to return to the utilities window.
10. If you want to start up again from the disk you erased, select Reinstall macOS in the utilities window, then click Continue and follow the onscreen instructions to reinstall macOS.



The steps will vary slightly on Macs depending on which processor your Mac has, and potentially which update of MacOS it has.

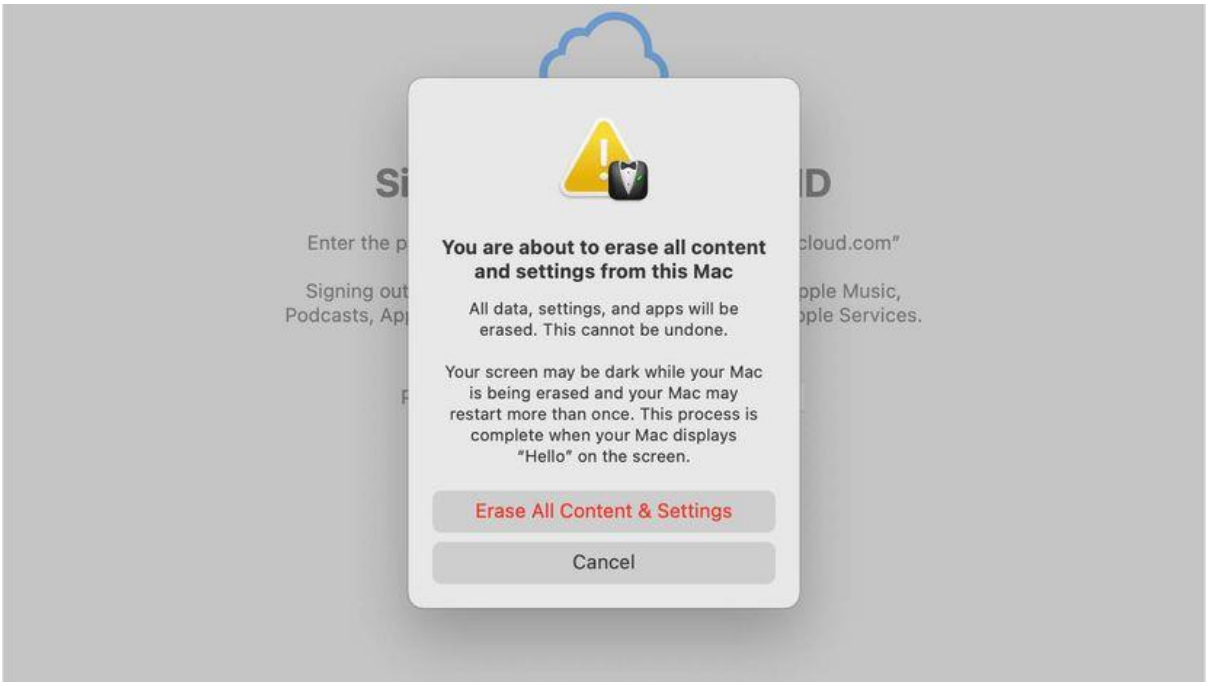
Apple

System Wipe, Silicon CPU

If your Silicon-based Mac is running a version of the OS pre-October 2021, follow these steps from Apple:

1. Turn on your Mac and continue to press and hold the power button until you see the startup options window. Select Options, then click Continue.
2. If asked, select a user you know the password for, then enter their administrator password.
3. If asked, enter the Apple ID and password previously used with this Mac.
4. From the utilities window, select Disk Utility and click Continue.
5. In the Internal section of the Disk Utility sidebar, make sure that you see the volume named Macintosh HD.

6. If you previously used Disk Utility to add volumes to your startup disk, select each additional internal volume in the sidebar, then click the delete volume (–) button in the toolbar to delete that volume.
7. During this step, disregard any internal volume named Macintosh HD or Macintosh HD - Data, as well as any volumes in the External and Disk Images sections of the sidebar.
8. Now select Macintosh HD in the sidebar.
9. Click the Erase button in the toolbar, then specify a name and format: Name: Macintosh HD Format: APFS or macOS Extended (Journaled), as recommended by Disk Utility
10. Click Erase. However, if you see an Erase Volume Group button, click that button instead.
11. If asked, enter your Apple ID.
12. When asked whether you're sure you want to erase this Mac, click Erase Mac and Restart.
13. When your Mac restarts, follow the onscreen instructions to choose your language.
14. Your Mac now attempts to activate, which requires an internet connection. Use the Wi-Fi menu in the menu bar to choose a Wi-Fi network, or attach a network cable.
15. After your Mac activates, click Exit to Recovery Utilities.
16. If you want to start up again from the disk you just erased, select Reinstall macOS in the utilities window, then click Continue and follow the onscreen instructions to reinstall macOS.



Be sure you have a backup of all the files you want to keep before you click erase!

Apple

System Wipe, Monterey Update

If your MacOS was updated after October 2021, follow these steps from Apple:

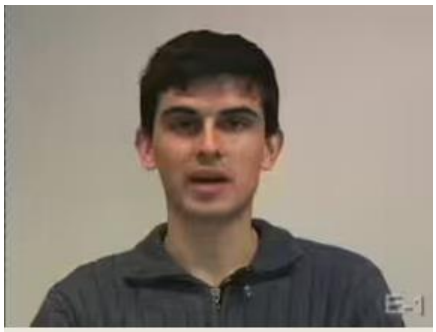
1. From the Apple menu in the corner of your screen, choose System Preferences.

2. From the System Preferences menu in the menu bar, choose Erase All Content and Settings.
3. Erase Assistant opens and asks you to sign in with your administrator credentials. Enter the password you use to log in to your Mac, then click OK.
4. Click Continue to allow your settings, media, data, and the other listed items to be removed.
5. If you're asked to sign out of Apple ID, enter your Apple ID password and click Continue.
6. Click Erase All Content & Settings to confirm that you want to proceed.
7. Your Mac restarts and shows a black screen or progress bar. If it needs to reconnect to a Bluetooth accessory such as a keyboard or mouse, you might be asked to turn on the accessory. If the accessory doesn't connect within 30 seconds, turn the accessory off and back on. When reconnecting to a Bluetooth keyboard, you're asked to choose a language.
8. You might be asked to select a Wi-Fi network or attach a network cable. To select a Wi-Fi network, use the Wi-Fi menu in the upper-right corner of the screen.
9. After joining a network, your Mac activates. Click Restart.
10. After restart, a setup assistant guides you through the setup process, as if you're setting up your Mac for the first time.

With your old device wiped clean, you can now pass it on to a new owner with confidence that data is gone and can't be lifted.

5 Everyday Things You Can Do to Keep Your Computer Healthy

By: Jacob Clifton



Learn how to practice safe computing.
HARVARD EXTENSION SCHOOL'S
COMPUTER SCIENCE E-1: UNDERSTAND

Hygiene is important! Most of us have it under control for ourselves, but for a lot of our technology, it's a bit messier under the hood. Just like keeping your house clean or brushing your teeth addresses problems before they can start, a little prevention of common computer problems can save you hours and dollars down the road. And, as with any intimidating situation, even a little foreknowledge and preparation can be vastly empowering.

For complicated machines like our cars, computers and gadgets, it's easy to be overwhelmed. It's not that we're being walled off from that knowledge at all -- they're our machines, we should know how to work with them, and the information is readily available -- but it can sometimes feel like an episode of "House" in there: Change one thing over here, and suddenly it's going haywire in a completely different area. So we tend to just shrug and keep going, even though our tech could work better than it does.

If you think about how much of your daily life is spent working with, or deriving benefit from, your desktop or laptop computer, that can be scary all on its own. It's a catch-22, in a way: We don't want to mess with our computers because we don't want to cause problems, so we treat the back end like a room we never go into ... which causes problems! Not everybody can be a DIY mastermind -- I'm certainly not one -- but with a few simple routines and tips, you can keep your computer's works as clean as a whistle without ever feeling like you've crossed the line or permanently ruined everything.

In this article, we'll look at the best ways to keep your machine working smoothly and quickly without breaking your budget -- or causing more problems as you learn.

Contents

1: Keeping It Cool

Check to make sure your cooling fans get adequate air circulation.
©JUPITER IMAGES/THINKSTOCK

Most of us understand that computers need to stay cool, theoretically. But the convenience of a laptop and the reliability of a desktop make it easy to forget to keep this idea in play. The desktop lives in its own special place, wherever that may be, and we go to it when we need to do something. It's easy to forget all the environmental issues that could be going on in there.

First, you want to ensure that there's plenty of airflow around all sides of the computer, especially the back on a desktop and often the bottom and sides for a laptop. While it's easy to declutter your desk or work area, it's also important to remember this tip if your tower lives under your desk, or in a special cubby, because the hot air in those situations can build up and recycle itself, getting hotter and hotter inside the space. Keep the cabinet doors open, for example, or take off the cubby's back panel to ensure proper flow.

You might have heard, or intuited, that taking the case off your computer is a good idea in cases of overheating. That's actually incorrect, because the case around your computer's guts is there to protect it from dirt and fuzz, which is one of the most common causes of overheating. Dust, pet hair, and all the rest of the daily grime are the biggest cause of PC temperature issues, because they interfere with the fans meant to cool your equipment down. If you've ever cracked a case open and looked at the fans inside, you won't have forgotten that grungy sight. Case closed, please.

Which leads us to the most helpful way to be proactive here: by cleaning and/or replacing the fans that keep everything working. While expensive solutions like water-cooling kits and phase-change units (imagine a high-end deep freeze for your machine) aren't necessary for the average computer, you can easily install extra fans for components inside the machine that are getting too excited for their own good. Chances are, whatever fans came pre-installed are not top of the line anyway, so if you're running into repeat issues on this front you might look into extra, or better, fans.

They're easy to spot: There's going to be one on the CPU, one inside the power supply, and probably another one on the front or side of the case itself. Just turn the computer off, take it outside, and clear those fans out with some canned air before deciding whether to upgrade. It's going to be nasty, but it's also pretty satisfying once you've gotten things clean again.

2: Powering UPS

Electrical outlets seem like a pretty simple proposition: You plug your stuff into them, and they work. (Even when you travel to other countries, with a little help.) But what we're not seeing our computers deal with is the little blips and interruptions coming out over the grid, all the time. Your average computer sold in the U.S. is meant to work off 120-volt AC power, oscillating at 60 Hz, but often that's not exactly what it's getting. Even if you never see the effect of those slip-ups and surges, the spikes and sags and tiny little brown-outs, the millisecond bumps in oscillation, your computer is feeling them.

The Institute for Electrical and Electronic Engineers tells us the typical AC outlet in North America gets a surge more than 600v (that's five times what your computer wants, and twice as much as what's dangerous to the equipment) about 13 times daily, and one more than 3000v (10 times the recommended maximum) about three times a week.

In fact, it's estimated that 47 percent of computer problems can be traced back, eventually, to this so-called "dirty power" [source: Superuser] An Uninterruptible Power Source, or UPS, is designed to keep the power coming steadily and constantly, even in the face of a total power outage, by using a battery and modulation system to filter the electric power. Essentially, it means your computer is always running off the UPS's battery, which the UPS is always recharging. That means there's no switchover time, like you'd imagine with a generator or other backup.

If you're convinced, just remember to keep your UPS grounded, replace the battery every three years -- you can get the replacements when you buy the unit, for convenience's sake -- and don't plug your printer or any other external devices into it. And, as is often recommended, it's probably a good idea to let the battery completely die at least a few times a year and recharge it from baseline.

3: Routine Software Checks

A good antivirus program will update frequently so it keeps the most current information on potential threats. ©ISTOCKPHOTO.COM/ROB BROEK

There are three utilities you should get to know, even if that's as far as you want to go with the man behind the curtain: defragmentation, disk checks and an antivirus program. Most of the free antivirus software we'll be looking at comes bundled with analogues of the other two -- as well as a version of the very helpful task scheduler we'll talk about later -- so we'll focus there, but here are some definitions for the layman. What these terms refer to is the wilderness of digital energy inside your computer's memory drives, which are naturally a lot less tidy than you might expect.

Defrag. Whenever you change, move, copy or delete a file, your computer usually does the minimum work necessary to give you the desired result. That means bits and pieces of files are left around in the empty spaces, not useful but also not gone, meaning your "free" space isn't technically free. A defrag utility will go hunting through the wilds of your free space, collecting those random shadows and getting rid of them for good. This frees up space your computer didn't even know it had, as well as speeding up the machine by pushing all the data that still matters into a more compact area of the disk so that your CPU doesn't have to hunt around for the various pieces of stuff you still care about, mixed in with the trash.

Immensely satisfying, whether you -- like me -- simply prefer things clean and elegant, are paranoid about leftover data, or just want to make everyday tasks easier and faster for your machine. (You will have to clear out at least 15 percent of the space on the drive before it can work, so if your problem is an over-full memory, you'll need to delete some stuff before it can give you the extra space.)

Chkdsk. Hand-in-hand with the defrag utility is this holdover from the early DOS days. It's a brute-force way of checking disks for errors, and it's the kind of thing you don't think about until about five minutes too late. If you don't use a sector of the disk -- or it's been left to the shadows, as above -- you might never know it's troubled until the computer tries to save something there. That's why Defrag usually includes or requires Chkdsk before it starts sorting through your leftovers. Just remember that a disk check requires exclusive access to the volume (For example, "C:" drive) before it starts, so you might have to go play on your phone or tablet for a while.

Antivirus. Of course, we all get into trouble. Even if we're not doing anything particularly shady or questionable, viruses get in: That's what they're made for. You need a solid watchdog program, but you'll also want something you can use for analysis when you're feeling suspicious or nervous about

the way something's acting. We judge antivirus software by three things: how much malware and viruses a program can detect, how good it is at getting them out of there without a trace or secondary issues, and how much memory and power they take up.

There are some great free programs on the market that excel in all three areas. The most popular ones are self-updating, meaning they're always learning new red-flags and ways of locating and immunizing against threats, they include utilities like those listed above so you can clean house all from one location (very satisfying), and they include task schedulers that can make all of these things happen while you're asleep!

4: Back It Up!

One easy way to remember your backup system -- which is to say, remember to actually use it -- is to remember that World Backup Day comes just before April Fool's Day, and that's no mistake. A lot of us are moving into the cloud these days, keeping our information and media online and accessing or streaming it at-will.

But if your needs are different -- if you have lots of data or media you want to keep to yourself, protect, or otherwise maintain access to regardless of equipment failure -- you really should listen to your IT guy and back that stuff up. (You also should have a backup system for all your important files you keep in the cloud.) While external hard drives have become easy to come by, there are plenty of services that provide storage, free or for a price, that can sync your data easily and seamlessly, so that you never have to worry about another crash or disaster.

Questions you should use to guide this search for the perfect match for your needs: How does the syncing work, and how often does it happen? Can you share the data with other people or computers? Can you access your data over the Web? Does it cover more than one computer? How about more than one type? Can you get a plan for both Macs and PCs at once? And how much is price a factor? You're going to be using gadgets other than your desktop or laptop more and more, if you don't already: You may need phone access or tablet access in the future that you don't need now, and the hassle of moving large storehouses of information can quickly be a real drag.

While many of the larger companies cater to a certain kind of paranoia -- as a sales tactic, of course -- these questions still matter, because you need to find the perfect backup service for you. The information that is most important to you will be just as important, at the end of the day, regardless of what you decide here. But in terms of your computer's health, and your own peace of mind, this is a comparison-shopping situation that could end up meaning a great deal down the road. Think about it this way: The more time you spend making the best choice now, the more likely you are to actually use the service, which is the end goal.

5: Common Sense Prevention

One of the best things you can do for computer maintenance is to become a savvy Web surfer. Don't shop at or download from questionable sites.
©DIGITAL VISION/THINKSTOCK

And then, of course, comes the lecture. You've been through all the nooks and crannies, you've blown out our fans and backed up our hard drives, you've cleaned up your registries and defragged, and even set timers for all this stuff in case it turns out to be less fun -- or memorable -- than I've made it seem. (Imagine your computer's upkeep utilities as a digital Mary Poppins, cleaning up the whole place with an electronic snap of her fingers!)

But none of that is going to help you if you walk right into the same old digital traps. Hygiene and preventive care are fine for mistakes, but that's only assuming you don't go looking for trouble. Music downloads, the Petri dish of peer-to-peer sharing, malware sites you didn't even mean to open, e-mail forwards from your kindly aunt, or well-disguised Trojan horse e-mails: They all happen to the best of us, whether or not we know what we're doing.

That's why you still need to take these threats seriously. There is no installable antivirus program available to protect you from yourself. That means being smart about torrents, downloads, adult sites and file sharing programs, but also taking advantage of protections that are already built into your computer and other programs.

Your browser has safety settings that have nothing to do with content and everything to do with suspicious code -- in fact, some more progressive browsers will even throw up a gateway before you reach some sites, just to make sure it's a trustworthy place to be. If you download a song or movie file and it tells you to download a new plug-in or codec, go get those things yourself instead of simply clicking "yes." Stay away from warez, cracks and serial number generators or downloaders -- all of those are potential danger zones. And most of all, make sure that anybody using your computer is either aware of the dangers, or that you've put measures in place to keep it safe. A lot of us can be confident about our savvy on these topics, but that doesn't extend to other folks using your machine.

In the end, knowledge really is power. But just because you shouldn't be afraid of your computer doesn't mean you shouldn't be wary of jerks, pet hair, or the million other things that could slow down your fun.

Lots More Information

Author's Note: 5 Everyday Things You Can Do to Keep Your Computer Healthy

I don't know about you, but I only tend to think about things like defragmenting or doing virus checks when I'm already past deadline or otherwise frustrated -- it's easier to blame my computer's performance than my own poor time management skills! Luckily, running a quick scan or deleting old files is a great way to clear out the computer and take my mind off deadlines as they go whizzing past, all at the same time. I read a lot of reviews for different free error-check and antivirus programs, but for my personal use -- and I've never had a problem in 15 years of often risky business -- I prefer CC Cleaner and Spybot Search & Destroy (sites noted below).

Related Articles

- 6 Easy Ways to Keep Your Computer Cool Without Using Electricity

- How does a computer's Uninterruptible Power Supply (UPS) work?
- Top 5 Computer How-To Videos
- How To Keep Your Laptop Cool
- How to Defrag Your Hard Drive
- How to Avoid Spyware
- 10 Commandments for Keeping Your Windows 7 Computer Running Smoothly

More Great Links

- Microsoft Support, with explanation and walkthroughs for disk-checks and defragmentation
- CC Cleaner, which includes a very helpful and safe registry cleaner
- Spybot Search & Destroy, a powerful and oft-updated antiviral and task-timer

Sources

- Gordon, Whitson. "How to Back Up Your Computer". Lifehacker, June 2011. (Sept. 21, 2012) http://lifehacker.com/5816453/how-to-back-up-your-computer
- Ho, Erica. "How to Prevent Your Computer from Overheating (and Why It's Important)". Lifehacker, June 2010. (Sept. 21, 2012) http://lifehacker.com/5570909/how-to-prevent-your-computer-from-overheating-and-why-its-important
- Howlett, Glenn. "What is the best antivirus software?" PC World Australia, Mar 2011. (Sept. 21, 2012) http://www.pcworld.idg.com.au/article/381521/what_best_antivirus_software_/
- Javali, Zahid H. "Tips for Buying a UPS". PC Mech, Oct. 2007. (Sept. 21, 2012) http://www.pcmech.com/article/tips-for-buying-a-ups/
- Johnson, Dave. "Pick the Right Size UPS for Your PC, Avoid Catastrophe When the Power Fails". CBS News, July 2009. (Sept. 21, 2012) http://www.cbsnews.com/8301-505143_162-28644399/pick-the-right-size-ups-for-your-pc-avoid-catastrophe-when-the-power-fails/
- Mac Xperts. "UPS (Uninterruptible Power Supply): How to Choose the Right UPS". The Mac Xperts Blog, Apr 2010. (Sept. 21, 2012) http://www.themacxperts.com/blog/files/4aa04d20befb92af9d7db54e376d4ad2-30.html
- Mediati, Nick. "Free Antivirus You Can Trust". PC World, Apr 2012. (Sept. 21, 2012) http://www.pcworld.com/article/254121/free_antivirus_you_can_trust.html
- Muchmore, Michael. "Disaster-Proof Your Data with Online Backup". PC Magazine, 30 Mar 2012. (Sept. 21, 2012) http://www.pcmag.com/article2/0,2817,2288745,00.asp
- Pot, Justin. "The 10 Best Free Anti-Virus Programs". MakeUseOf, Apr 2010. (Sept. 21, 2012) http://www.makeuseof.com/tag/ten-best-antivirus-programs/
- Rubenking, Neil J. "The Best Antivirus for 2012". PC Magazine, Aug 2012. (Sept. 21, 2012) http://www.pcmag.com/article2/0,2817,2372364,00.asp

Why Is My Computer So Slow? 5 Reasons and How to Fix Them

By: Dave Roos | Updated: Mar 5, 2024

A slow computer may be due to several different factors. Prostock-studio/Shutterstock

Few things interfere with work and play quite like a slow computer. Fortunately enough for those wondering, "**Why is my computer so slow**?" answers and solutions aren't far away.

Everyone has been there. After a long day of browsing, streaming and switching between multiple applications, even the most loyal computer may exhibit symptoms of fatigue: the fan blows nonstop, applications start to freeze or crash, and everything from loading websites to saving documents slows to an excruciating crawl.

But why is your computer running slow and what can you do about it? We put a call out to tech experts and serious hobbyists for the top reasons why computers start to bog down and the easiest fixes to get your machine humming again.

Contents

1. The RAM Is Running Out

Having enough random access memory (RAM) is super important for a smoothly functioning PC or laptop. RAM is your computer's short-term memory, temporarily storing files that need to be quickly accessed by your computer's processor or central processing unit (CPU).

"Some software and applications require a lot of resources, especially when these programs run in the background and have an auto-update mechanism," says Nick Murphy, co-founder and editor at Techozu, in an email. "If a program is silently updating in the background, it's going to slow down the computer."

Every application that's open on your computer is competing for memory and processing power. That includes background processes, individual browser tabs on Chrome or Safari, music being streamed on Spotify and antivirus programs scanning for bugs. When RAM starts to run out, it overwhelms your CPU and programs will slow down, freeze or crash entirely.

The Fix: The first step is to close any unnecessary applications. If you're not sure what's open and running on your computer, there's an easy way to check:

- In Windows, open the Task Manager by typing Ctrl+Alt+Del
- On a Mac, go to your Applications folder > Utilities folder, and then double-click on Activity Monitor
- On a Chromebook, click the three dots in the top right of any browser window > More tools > Task manager

With all three of those tools, you can see which applications are hogging the most RAM and CPU power and close them. If you see a bunch of startup programs running that you don't use very often, make sure that they're not opening automatically each time you start your computer.

"If you have too many programs set to start up automatically when your computer starts, it can slow down the boot process and make your computer run slow," says Jeroen Van Gils, founder of Lifi.co in an email. "To fix this, you can go into your startup settings and disable any programs that you don't need to start automatically."

Also, how many browser tabs do you have open at once? Browser tabs might not seem like a big deal, but each one eats up RAM. If you have 10, 20 or more tabs open at once (which can easily happen with multiple browser windows), that's going to slow your computer down.

Lastly, if your computer is more than four years old or a bargain model, you simply might not have enough RAM to run newer, memory-hungry applications.

"All of the programs, applications, games, etc. are improving all the time, and they require more powerful devices to run smoothly," says Phil Vam, tech expert and owner of Majordroid in an email. "I know that many people think 4GB of RAM is enough, but realistically, smartphones have more RAM nowadays. In my opinion, 8GB of RAM is the minimum, while 16GB of RAM is ideal for 99 percent of users."

2. The Hard Drive Is Maxed Out

We tend to think of the hard drive as the computer's long-term memory, which is true, but the hard drive isn't exclusively used for permanent data storage. Your hard drive also stores temporary files that help applications run smoothly.

One of the most common reasons a computer runs slowly is that the hard drive is nearly full. "Keep at least 20 percent of hard disk drive (HDD) space empty for smooth processing," says Levon Galstyan, a serious computer hobbyist who works for the Oak View Law Group. "Almost-full HDDs cannot work properly."

The Fix: To free space on your computer, delete temporary files, uninstall any rarely used applications and consider storing really big files in the cloud. If you have a Mac, for example, you might want to save all your photos and videos in iCloud (you get 5GB of storage for free but can pay for more). Microsoft offers a similar cloud solution for Windows users called OneDrive, and so does Google, which gives you 15GB of free storage.

And then there's the underlying technology of your computer's hard drive. Older hard drives use a spinning disk to write and store data, but over time that can lead to errors and performance issues.

"The term 'fragmentation' refers to the phenomenon in which your files are dispersed over your hard disk rather than being kept in a single, logical location," says Adam Crossling, head of marketing at IT support service Zenzero, in an email. "Your computer's performance may suffer if it has trouble accessing critical data."

If you have one of those disk-based hard drives, you will need to "defrag" it from time to time to reorganize the data, but all of the experts we consulted recommended switching from an old-school disk drive to a solid-state drive (SSD), which doesn't get fragmented.

3. The Software Is Outdated

Every time Apple or Microsoft releases the latest version of their operating systems, all of the marketing hype focuses on cool new features and functionality, but there's far less buzz about all of the updates that come out in between those big releases.

"Those updates, however, are often the most important," says Jeremy Clifford, CEO of RouterCtrl, in an email. "[Operating system updates] feature security patches and performance fixes, all of the things that can make your computer run like molasses in the winter."

The Fix: Here's how to check if you have the latest version of your operating system:

- For a Windows PC or laptop, click on the Start button, and then go to Settings > Update & Security > Windows Update
- On a Mac, open System Preferences and click on Updates
- On a Chromebook, click on the time, then the settings icon, then About ChromeOS

4. The Computer Has Viruses or Malware

Malware and viruses can often slow down your computer's performance. Kanoktuch/Getty Images

If your computer has been infected with some kind of virus or piece of malware (malicious software), that will definitely slow it down.

The Fix: All of our experts recommended running some kind of antivirus or antimalware software that routinely scans for suspicious files, bots and other unwelcome programs that run in the background and sap your precious RAM and processing power. But make sure to keep your antivirus program updated as well!

"[A] frequent cause for sluggish PCs and Macs is outdated antivirus software," says Abdul Rahim, founder of Software Test Tips in an email. "Unfortunately, these programs often create havoc by severely slowing down your system while trying to clean up after themselves."

5. The Computer Is Too Hot

If your PC's fan is running nonstop or the bottom of your laptop gets warm to the touch, those are signs that your computer is overheating. Not only can overheating damage the circuit boards and other computer hardware components over the long term, but it can also slow down performance.

That's because modern processors are programmed to automatically slow down when internal temperatures get too high, a precaution known as thermal throttling.

The Fix: Your computer's internal fans, vents and heat sinks should be able to keep the temperature down, but there are several things that you can do to avoid overheating. If you use a laptop, don't actually keep it on your lap or on a naturally insulating surface like the comforter of your bed. That will trap in the heat.

A dirty computer is also a hot computer. When dust builds up inside your computer's vents, it can prevent the fans from working properly and trap heat inside.

But you can clean it. If you have a PC, open it up, get a can of compressed air and clean out the fans, ducts, and other components. If necessary, do a deep clean by adding isopropyl alcohol to a cotton swab or cloth for the more delicate parts of the computer.

Now That's Cool

To keep your computer healthy, invest in an all-in-one PC "cleaner" or "optimizer" program that will scan for viruses, delete temporary and junk files, optimize your hard drive, and automatically update drivers and utility software. Many cleaners are free for the basic version or offer you a free trial.

Why Is My Computer So Slow? 5 Reasons and How to Fix Them

By: Dave Roos | Updated: Mar 5, 2024

A slow computer may be due to several different factors. Prostock-studio/Shutterstock

Few things interfere with work and play quite like a slow computer. Fortunately enough for those wondering, "**Why is my computer so slow**?" answers and solutions aren't far away.

Everyone has been there. After a long day of browsing, streaming and switching between multiple applications, even the most loyal computer may exhibit symptoms of fatigue: the fan blows nonstop, applications start to freeze or crash, and everything from loading websites to saving documents slows to an excruciating crawl.

But why is your computer running slow and what can you do about it? We put a call out to tech experts and serious hobbyists for the top reasons why computers start to bog down and the easiest fixes to get your machine humming again.

Contents

4. The Computer Has Viruses or Malware
5. The Computer Is Too Hot

1. The RAM Is Running Out

Having enough random access memory (RAM) is super important for a smoothly functioning PC or laptop. RAM is your computer's short-term memory, temporarily storing files that need to be quickly accessed by your computer's processor or central processing unit (CPU).

"Some software and applications require a lot of resources, especially when these programs run in the background and have an auto-update mechanism," says Nick Murphy, co-founder and editor at Techozu, in an email. "If a program is silently updating in the background, it's going to slow down the computer."

Every application that's open on your computer is competing for memory and processing power. That includes background processes, individual browser tabs on Chrome or Safari, music being streamed on Spotify and antivirus programs scanning for bugs. When RAM starts to run out, it overwhelms your CPU and programs will slow down, freeze or crash entirely.

The Fix: The first step is to close any unnecessary applications. If you're not sure what's open and running on your computer, there's an easy way to check:

- In Windows, open the Task Manager by typing Ctrl+Alt+Del
- On a Mac, go to your Applications folder > Utilities folder, and then double-click on Activity Monitor
- On a Chromebook, click the three dots in the top right of any browser window > More tools > Task manager

With all three of those tools, you can see which applications are hogging the most RAM and CPU power and close them. If you see a bunch of startup programs running that you don't use very often, make sure that they're not opening automatically each time you start your computer.

"If you have too many programs set to start up automatically when your computer starts, it can slow down the boot process and make your computer run slow," says Jeroen Van Gils, founder of Lifi.co in an email. "To fix this, you can go into your startup settings and disable any programs that you don't need to start automatically."

Also, how many browser tabs do you have open at once? Browser tabs might not seem like a big deal, but each one eats up RAM. If you have 10, 20 or more tabs open at once (which can easily happen with multiple browser windows), that's going to slow your computer down.

Lastly, if your computer is more than four years old or a bargain model, you simply might not have enough RAM to run newer, memory-hungry applications.

"All of the programs, applications, games, etc. are improving all the time, and they require more powerful devices to run smoothly," says Phil Vam, tech expert and owner of Majordroid in an email. "I know that many people think 4GB of RAM is enough, but realistically, smartphones have more RAM nowadays. In my opinion, 8GB of RAM is the minimum, while 16GB of RAM is ideal for 99 percent of users."

2. The Hard Drive Is Maxed Out

We tend to think of the hard drive as the computer's long-term memory, which is true, but the hard drive isn't exclusively used for permanent data storage. Your hard drive also stores temporary files that help applications run smoothly.

One of the most common reasons a computer runs slowly is that the hard drive is nearly full. "Keep at least 20 percent of hard disk drive (HDD) space empty for smooth processing," says Levon Galstyan, a serious computer hobbyist who works for the Oak View Law Group. "Almost-full HDDs cannot work properly."

The Fix: To free space on your computer, delete temporary files, uninstall any rarely used applications and consider storing really big files in the cloud. If you have a Mac, for example, you might want to save all your photos and videos in iCloud (you get 5GB of storage for free but can pay for more). Microsoft offers a similar cloud solution for Windows users called OneDrive, and so does Google, which gives you 15GB of free storage.

And then there's the underlying technology of your computer's hard drive. Older hard drives use a spinning disk to write and store data, but over time that can lead to errors and performance issues.

"The term 'fragmentation' refers to the phenomenon in which your files are dispersed over your hard disk rather than being kept in a single, logical location," says Adam Crossling, head of marketing at IT support service Zenzero, in an email. "Your computer's performance may suffer if it has trouble accessing critical data."

If you have one of those disk-based hard drives, you will need to "defrag" it from time to time to reorganize the data, but all of the experts we consulted recommended switching from an old-school disk drive to a solid-state drive (SSD), which doesn't get fragmented.

3. The Software Is Outdated

Every time Apple or Microsoft releases the latest version of their operating systems, all of the marketing hype focuses on cool new features and functionality, but there's far less buzz about all of the updates that come out in between those big releases.

"Those updates, however, are often the most important," says Jeremy Clifford, CEO of RouterCtrl, in an email. "[Operating system updates] feature security patches and performance fixes, all of the things that can make your computer run like molasses in the winter."

The Fix: Here's how to check if you have the latest version of your operating system:

- For a Windows PC or laptop, click on the Start button, and then go to Settings > Update & Security > Windows Update
- On a Mac, open System Preferences and click on Updates
- On a Chromebook, click on the time, then the settings icon, then About ChromeOS

4. The Computer Has Viruses or Malware

Malware and viruses can often slow down your computer's performance. Kanoktuch/Getty Images

If your computer has been infected with some kind of virus or piece of malware (malicious software), that will definitely slow it down.

The Fix: All of our experts recommended running some kind of antivirus or antimalware software that routinely scans for suspicious files, bots and other unwelcome programs that run in the background and sap your precious RAM and processing power. But make sure to keep your antivirus program updated as well!

"[A] frequent cause for sluggish PCs and Macs is outdated antivirus software," says Abdul Rahim, founder of Software Test Tips in an email. "Unfortunately, these programs often create havoc by severely slowing down your system while trying to clean up after themselves."

5. The Computer Is Too Hot

If your PC's fan is running nonstop or the bottom of your laptop gets warm to the touch, those are signs that your computer is overheating. Not only can overheating damage the circuit boards and other computer hardware components over the long term, but it can also slow down performance.

That's because modern processors are programmed to automatically slow down when internal temperatures get too high, a precaution known as thermal throttling.

The Fix: Your computer's internal fans, vents and heat sinks should be able to keep the temperature down, but there are several things that you can do to avoid overheating. If you use a laptop, don't actually keep it on your lap or on a naturally insulating surface like the comforter of your bed. That will trap in the heat.

A dirty computer is also a hot computer. When dust builds up inside your computer's vents, it can prevent the fans from working properly and trap heat inside.

But you can clean it. If you have a PC, open it up, get a can of compressed air and clean out the fans, ducts, and other components. If necessary, do a deep clean by adding isopropyl alcohol to a cotton swab or cloth for the more delicate parts of the computer.

Now That's Cool

To keep your computer healthy, invest in an all-in-one PC "cleaner" or "optimizer" program that will scan for viruses, delete temporary and junk files, optimize your hard drive, and automatically update drivers and utility software. Many cleaners are free for the basic version or offer you a free trial.

How to Get Rid of a Virus on a Windows PC

By: Jonathan Strickland & Desiree Bowie | Updated: Jul 30, 2024

Learning how to remove viruses from your computer can make alarming error screens a little less scary. Muharrem huner / Getty Images

We all know malware is out there — applications that spy on you, corrupt your data, destroy your hard drive or give control of your machine to someone thousands of miles away.

Since there are many examples of malware in the wild, it may only be a matter of time before you become the victim of a malware attack. When that happens, you'll need to know **how to get rid of a virus** or any other type of malicious software that may be infecting your PC.

The most important advice we can give anyone who believes they have a computer with malware on it is this: Don't panic. Also, don't assume that you need to wipe your computer clean and start from scratch. Often, you can remove malware without having to erase everything else. You may lose some data in the process, but you probably won't lose everything.

Contents

Detecting a Computer Virus

First, you need to determine if your computer has a virus at all. Sluggish performance is a sign of malicious code. If your web browser suddenly looks different or automatically redirects to an unfamiliar site, that’s a good indication that malicious programs are at play.

Unstable behaviour, such as frequent crashes, can also signal a problem. Additionally, if you try to access files and receive messages saying they're corrupted, that's another red flag.

If you suspect your computer has a virus, run antivirus software to identify and remove it.

Antivirus software is practically a requirement for anyone using the Windows operating system. While it's true you can avoid computer viruses if you practice safe habits, the truth is that the people who create malicious apps and programs are always looking for new ways to infect computer systems.

A few malware variants will try to block you from downloading antivirus software. If that's the case, you may need to download the software on another computer and transfer it to disk or a flash drive.

If you don't have any antivirus software, now's a good time to purchase or download an application. There are several different antivirus programs on the market — some are free and some you have to purchase. Keep in mind that free versions often lack some of the nicer features you'll find in commercial products.

Removing Malware

Assuming your antivirus software is up to date, it should detect malware on your machine. Most antivirus programs have an alert page that will list each and every virus or other piece of malware it finds. Write down the names of each malware application your software discovers. (More on this in a bit.)

Many antivirus programs will attempt to remove or isolate malware for you. You may have to select an option and confirm that you want the antivirus software to tackle the malware. For most users, this is the best option; it can be tricky removing malware on your own.

If the antivirus software says it has removed the malware successfully, shut down your computer, reboot and run the software again. This time, if the software comes back with a clean sweep, you're good to go.

If the antivirus software finds different malware, repeat the previous steps. If it finds the same malware as before, you might have to try something else.

Two's a Crowd

If one antivirus program is good, two is better, right? Wrong. This type of software tends to use up a large percentage of the processing power of your computer system.

Running more than one antivirus program will slow your computer to a crawl and possibly cause it to crash. Not all antivirus programs are compatible with one another, which can make your computer even more unstable.

Advanced Tips for Computer Virus Removal

If you can't access your antivirus software or keep seeing the same malware pop up scan after scan, start your computer in Safe Mode. Many computer viruses store files in your Windows registry folder, which acts like a database of instructions and tells your operating system important information about the programs on your computer.

It can also tell viruses to activate as soon as the operating system loads. Starting your computer in Safe Mode allows you to work with your machine using only the core elements of the Windows OS.

Try running your antivirus software in this mode. If new malware is detected, you may have found a solution. Some malware exists solely to download and install other malware on your machine. Removing all these applications can significantly improve your system's security.

Research the Malicious Software

If your antivirus software can't remove the virus on its own, additional research is needed for manual removal. You've already written down the names of all the malware applications that your software discovered. Now it's time to research each of those files online using the same internet security firm that produced your antivirus software.

Different firms sometimes give the same virus different names, so using the same firm's resources ensures consistency. Most internet security firms list all the files associated with a particular virus and indicate where to find them. You may need to search extensively to locate each file.

Before deleting any files, save a backup copy of your registry folder. Accidentally deleting the wrong file can make it difficult or impossible to run your computer properly.

Now delete all the infected files associated with the malware on your list. Once that's done, reboot your computer and run your antivirus software again. Hopefully, nothing else will be detected.

Finally, update your login information for your various online accounts. Some malware includes keylogging software that can send your passwords and other information to a remote user. It's better to be safe than sorry.

Give Viruses the Boot (Disk)

Some antivirus software allows you to create a special boot disk. This disk can be invaluable when your computer is infected with particularly stubborn malware that prevents normal operation. The boot disk enables you to start your computer from a clean, secure environment, bypassing the infected operating system.

After creating a boot disk, reboot your computer with the disk in the drive. Your computer will read from the disk, load a limited operating system, and run a virus scan. This method can help you bypass the malware's code and disable it, effectively removing the infection and restoring your system to a functional state.

How to Avoid Computer Viruses

To avoid computer viruses on a Windows computer, follow these simple guidelines that mostly rely on common sense:

1. **Practice e-mail safety.** Do not open strange email attachments or click on hyperlinks in e-mails from unknown sources. Virus programmers often use these tactics to distribute malicious software. Only click on hyperlinks if the sender provides a clear description of the link and its destination.
2. **Disable auto-launch.** If your email client supports auto-launch, turn it off. This feature can automatically activate a computer virus just by opening an e-mail.
3. **Be cautious with messages.** Be wary of hyperlinks in message boards, Facebook messages or instant messages. Pay attention to the source of the message and look for unusual signs like misspellings or odd sentence structures, especially if the sender usually avoids such errors.

4. **Avoid questionable websites.** Refrain from visiting websites that are known for hosting malware, such as those related to software, music and video piracy or adult content. Modern web browsers often warn you if you attempt to access such sites — heed these warnings.
5. **Use pop-up vigilance.** Pay attention to any pop-up windows while browsing the web. Be cautious of notifications claiming that you need to download the latest video driver or other software to view content. This is a common method for distributing malware.
6. **Perform regular maintenance.** Run your antivirus or internet security software at least once a week. Ensure your software and operating system are up to date by regularly downloading updates and patches. Most antivirus programs update at least once a week as security firms add new virus information to their databases.
7. **Clear temporary files.** Regularly clear your computer's temporary files to prevent malware from exploiting them.

Worst-case Scenario

If you cannot delete a malware infection despite trying various methods, it might be time to perform a complete system wipe on the infected computer. This involves formatting your hard drive and reinstalling the operating system.

A complete system wipe is often a last resort because it will delete all of your information, including programs, settings and personal files. Therefore, it is crucial to back up any important, virus-free files before you start. You can use external storage devices or cloud services for this purpose.

Performing a system wipe can be time-consuming, as you will need to reinstall the operating system, update it, reinstall all your applications and restore your data. However, this method ensures that all traces of malware are removed, giving you a fresh start with a clean slate.

After a system wipe, it is essential to immediately install antivirus software and update it to the latest version to protect your newly restored system from future infections.

This article was updated in conjunction with AI technology, then fact-checked and edited by a HowStuffWorks editor.

Lots More Information

Sources

- Academic Computing. "What to do if your computer is already infected with a virus." University of Minnesota. (March. 26, 2009) http://www1.umn.edu/adcs/guides/security/infection_cleanup.html
- Dittrich, David. "Lifecycle: Preventing, detecting and removing bots." March 20, 2005. (March 19, 2009) http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1068906,00.html
- Microsoft Security. "How to remove a computer virus." Microsoft. Dec. 31, 2008. (March 25, 2009) http://www.microsoft.com/protect/computer/viruses/remove.mspx
- Robertson, Jordan. "How to tell, what to do if computer is infected." AP News. March 15, 2009. (March 17, 2009) http://hosted.ap.org/dynamic/stories/T/TEC_INSIDE_A_BOTNET_CHECKLIST?SITE=ILEDW&SECTION=HOME&TEMPLATE=DEFAULT