

A lesson in backups

June 3 2016, by Troy Wolverton, The Mercury News

Michael Friedman learned the hard way how important it is to back up computers.

About 10 years ago, the hard drive on his wife's computer, where they kept all their family photos, died and the [data](#) wasn't backed up anywhere. Friedman, who lives in San Jose, sent the drive off to a data recovery service to try to salvage his pictures. He was lucky. He didn't lose anything, but it cost him a small fortune - somewhere in the neighborhood of \$2,000.

Friedman's sister-in-law wasn't so fortunate. About a year or two later, the hard drive on her computer crashed in such a way that the data on it wasn't recoverable. She ended up losing years of data, he said.

"She has no photos of the birth of her first son," said Friedman, 46, a software developer at Polyvore, which was recently acquired by Yahoo. "They were all on the hard drive that she lost. She can never recover those."

With smartphones and tablets sucking up more and more of our computing time, the humble PC may not get much attention these days. But even with cloud services proliferating, your PC likely contains your only copies of much of your most important and precious data, including your photos, music collection and financial and personal documents.

That data is at risk from any number of potential problems - not just hard drive crashes, but malware, theft, natural disasters and things as

mundane as coffee spills and user error. If you don't want to lose your data, you need to be prepared.

There are two kinds of people in the world, said Phil Goodwin, an analyst at tech research firm IDC who focuses on computer storage and data protection: "Those who have lost data and those who will lose data."

That may be a truism, but not everyone is convinced. Only about 10 to 20 percent of corporations have a formal plan in place to backup their employees' work PCs, Goodwin estimated. The portion of consumers who regularly backup their home computers is likely even lower, he said.

Count Steve Wright among those who don't regularly back up their data. Wright, a former journalist and communications executive, has some documents stored in Google Docs and photos spread across several external hard drives, but he doesn't have any kind of comprehensive back up of all his data.

He has worried about what might happen if his computer or drive were stolen or lost. But that's never happened. And he's never had a computer or drive fail on him. So he's never been particularly motivated to back up his data.

"I never wanted to take the time to do it," he said.

I was in a similar boat not that long ago. I'd backed up my data here and there but didn't do it regularly. I was worried about it but not enough to figure out a solution.

But then my computer was stolen, and I worried that I had lost for good a sizable portion of my photo library, including video of my daughter learning to ride a bike. Because I had saved my photos in a smattering of places and still had many stored on the SD card in my camera, I ended

up recovering almost everything, but I've been determined since to better and more thoroughly protect myself.

The problem with backups is that there are no perfect solutions. Instead, each has its own benefits and drawbacks.

Online backup services such as Mozy and Carbonite can be easy to use and will protect you if your computer is stolen or your house burns down. But they can be pricey and slow.

You can choose to back up to dedicated services, like saving all your photos to Google Plus or Flickr, your documents to Dropbox or Google Docs, and your music to iTunes Match or Amazon Cloud Music. But in many cases, you have to pay extra for those services. It may be difficult to recover your data from them. And some may compress your files in ways that can distort them.

You can also go the old-fashioned route and use an [external hard drive](#), which is relatively cheap, easy and fast. But if your computer gets infected with malware, it can compromise your backup disc as well. And if a disaster destroys your computer, it will likely wipe out your backup also.

So, after talking with backup experts, here's my advice: If you can afford it, choose more than one method. Or, as Richard Fisco, the test program leader for electronics at Consumer Reports, calls it, take the "belt and suspenders" approach.

Back up to a local hard drive and to a cloud service. Or back up to more than one external drive, one of which you store in a place away from your computer. Or save your most important files to Dropbox while doing a regular online backup.

But even backing up to just one place is better than nothing.

"That's better than what most consumers doing," said Stephanie Balaouras, an analyst who focuses on security and risk for Forrester, a tech research firm. "You're protecting your sensitive information, and you're saving yourself a whole lot of time."

—

PC Backup options

You have multiple options for backing up the data on your computer, but none is perfect solution.

Online backup. Services including Mozy, Carbonite and Crashplan will automatically back up your data so you don't have think about it. They often will save multiple versions of your files so if a file gets corrupted or you accidentally delete some information within it you can restore it from an earlier copy. Because your backups are data in the cloud rather than in your home, you're protected from things like the theft of your drive or an earthquake that might damage it.

But your initial backup to an online service can frequently take days or even weeks, depending on how much data you're saving and the speed of your Internet connection. If you have to restore your entire hard drive from the service over the Internet, you can expect a similarly lengthy amount of time. In some cases, when you need to recover your files, you can ask the [online backup service](#) to ship you out a hard drive with your data on it - but at a steep price. Depending on your Internet provider and the amount of data you're transferring, you may also see extra charges on your broadband bill for exceeding your data caps. And you may have to worry about your data getting hacked: the security of your backups may be only as good as the password you use.

Online storage. You can use services such as Google Photos to store pictures, Dropbox to store documents and Apple's iTunes Match to store your music. Many of these services offer at least basic storage for free and can automatically sync with files on your computer. But many such services charge extra for additional storage and some will compress your files to save space. Some also don't save multiple versions of your files or could allow them to be compromised if malware infects your computer.

External hard drive. Hard drives are relatively cheap these days, at least compared to how much you can store on them. Unlike an [online backup](#) service, once you buy an external drive, you don't have any ongoing cost. It's also typically much quicker to both back up to and restore from a [hard drive](#) that's in your house. And services like Time Machine on the Mac make it easy to automatically save multiple versions of your files.

But if a fire burns down your house, you'll likely lose not just your computer, but your backup too. An external drive that's always attached to your [computer](#) is at risk of being corrupted by malware. You can protect yourself by remembering to unplug it after each [backup](#) - but then you have to remember to plug it back in on a regular basis.

©2016 The Mercury News (San Jose, Calif.)
Distributed by Tribune Content Agency, LLC.

Citation: A lesson in backups (2016, June 3) retrieved 12 May 2024 from <https://phys.org/news/2016-06-lesson-backups.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
