COMPUTER NEWS from the

FEBRUARY 2015 Volume 3 NO.2

As found on the web and other sources

A friend of mine got one of these calls last week so I thought ti was worth-while repeating this warning!

Microsoft Sues Fake Tech Support Scammers

By Brandon Dimmel on December, 23 2014 in “Infopackets.com”.

Have you ever received a **suspicious phone call from someone claiming to work for Microsoft's technical support department**?

Late last week Microsoft announced that it had sued two technical support companies alleged to have infringed on several Microsoft trademarks. According to the firm, these companies called people at home offering support for non-existent problems with the Windows operating system. Microsoft says many people were tricked by the scheme and paid the scammers money for their assistance.

Scammers Claim to Represent Microsoft

"Defendants have utilized the Microsoft trademarks and service marks to enhance their credentials and confuse customers about their affiliation with Microsoft," Microsoft says in its complaint. "Defendants then use their enhanced credibility to convince consumers that their personal computers are infected with malware in order to sell them unnecessary technical support and security services to clean their computers." (Source: **computerworld.com**)

The two companies sued by Microsoft include California-based Customer Focus Services and Florida-based Anytime Techies. Microsoft says these firms used a range of sites -- including omnitechsupport.com, fixnow.us, anytimetechies.com, and windowssetgetsolution.org -- to support its fraudulent claims.

Windows Event Log "Malfunctions" Harmless

Microsoft says that, in most cases, people targeted by Customer Focus Services and Anytime Techies were told that their Windows-based systems were malfunctioning, often as a result of a malware infection. To demonstrate the existence of these issues, scammers pointed victims to the Windows Event Log, which shows processes and errors - most of which are harmless. That's when the caller, who claims to be a legitimate Microsoft support technician, attempts to convince the target to pay money for technical assistance.

The end result often involves the installation of useless software the scammers claim will resolve malware infections and other phantom problems with Windows, Microsoft says.

Undercover Microsoft Investigator Pays $860

In an effort to learn more about the scam, Microsoft carried out an investigation that involved calling the phone numbers listed through the websites associated with Customer Focus Services and Anytime Techies.

Once the connection was made, the scammers "claimed to have found 75 issues of concern ... caused by '**polymorphic viruses**,'" Microsoft said. "The alleged issues involved benign junk files and folders, none of which contained viruses or malware," the firm added. Nevertheless, the Microsoft investigator complied with the request. In the end, they paid $860 USD to "clean" and "fine tune" a Windows-based PC that Microsoft claims was healthy.

Overall, it's estimated these kinds of scams have generated annual revenue of $1.5 billion in the United States alone. (Source: **cnet.com**)

What's Your Opinion?

Have you ever been contacted by a suspicious caller claiming to represent Microsoft or another major tech company? Did you immediately hang up or did you try to learn more about the scam? What do you think the penalty should be if Microsoft wins its lawsuits?

COFFEE break time

Jailbreaking phones so you can do whatever you want with them is old news. Now you can jailbreak that fancy Keurig 2.0 coffeemaker so it will accept less expensive coffee pods made by third parties. Thanks to open-source coffee champion, Clark Howard!

If you don't have a FREE subscription to "Windows Secrets", get one. Fred Langa is just one of the contributors to this informative newsletter.

Mastering Windows 8's backup/restore system

By Fred Langa

Windows 8 has easily the most comprehensive backup-and-recovery system ever seen on a personal computer.

With little user effort, and when applied correctly, Win8's built-in backup tools provide automatic, frequent, triple-data redundancy.

Inexplicably, however, Microsoft tends to describe each tool more or less in isolation. It doesn't provide a simple, comprehensive explanation of how the backup components work together — and do so extremely well.

This article rectifies that deficiency; it describes how to use File History, OneDrive, and other options as a complete system for near-bulletproof backups.

You'll also find numerous links to articles that provide detailed how-to information — and operational tips on backing up Windows 8 systems.

An overview: Win8's three-part backup system

Here are the main components:

- **File History — Local backups of user data:** Win8's File History tool makes continuous, near-real-time, incremental backups of selected user files. It then stores these backups on a networked

or USB-attached external drive. If the primary copy (the working file) is damaged or accidentally erased, it can be quickly and easily restored from the local File History backups.

- **OneDrive — remote user-data backup:** Local backups are critical, but they have a potentially fatal flaw: any event that damages your PC or the drive containing your working files might also eliminate your local backups. Fires, floods, thefts, electrical surges, and similar catastrophes might result in the loss of ***all*** local copies. The answer for that possibility is cloud storage/backup, which maintains copies of your files on fully protected data servers, far removed from your PC.

  Microsoft's cloud-based storage service started out as the relatively simple SkyDrive. But over the past few years, Microsoft has steadily improved the service's capabilities, including tightly integrating it with Office 2013 and building it into Windows 8. (In fact, one of the early complaints about Office 2013 was its preference for storing files in SkyDrive.) Because of a trademark dispute, the service was renamed OneDrive in early 2014.

  There are, of course, many other cloud storage and backup services that will let you restore lost files. (A Nov. 20, 2014, Best Practices [paid content] discusses the differences between cloud-based synching and backup.) But — as is hardly discussed at all by Microsoft — OneDrive and File History can work cooperatively to provide automatic, double backups of all your important files.

  With almost no effort on your part, files can be automatically saved to three separate locations — the primary data drive, the external File History drive, and the OneDrive cloud — in near-real time. It virtually guarantees that you'll never lose an important file again!

  Why "important" files? By default, OneDrive users get 15GB of free online storage. Yes, you can put copies of ***all*** your data on OneDrive — but only if it amounts to fewer than 15GB or you're willing to pay for additional storage space. (Note: Office 365 subscribers get essentially unlimited storage [more info].)

- **OS backups and system imaging:** Windows 8 includes separate tools to back up and restore the operating system. **Refresh** lets you perform a nondestructive reinstall of the operating system while leaving most of your user files alone. However, not all user-installed, desktop applications will survive the process; you must use the **custom imaging** option to preserve your specific software setup. **Reset** does a full, clean-slate, factory restore.

With that foundation, we're ready to take a closer look.

How File History creates reliable local backups

As mentioned above, Win8's File History (Figure 1) is a highly automated, set-and-forget, near-real-time, archiving system. It does, however, ***require*** a drive other than the primary Windows (typically **C:**) drive. The backup drive can be a second internal disk, an external USB storage device, or a networked drive.

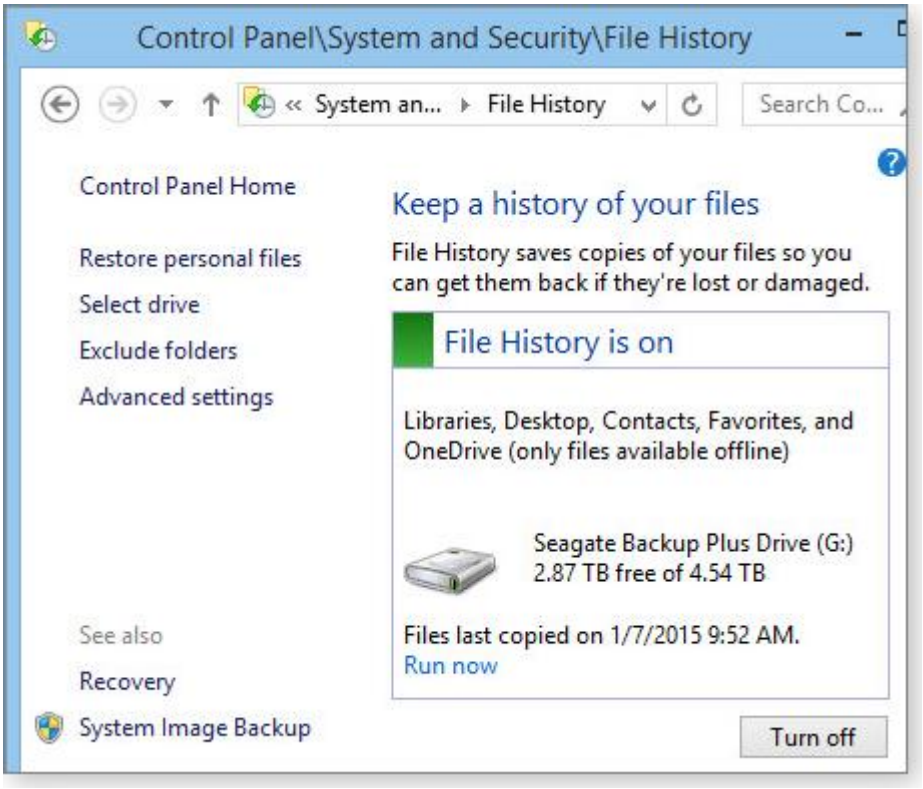

Figure 1. It's easy to access, configure, and fine-tune Win8's File History.

By default, File History automatically backs up everything in your Windows libraries — typically Documents, Music, Pictures, and Videos. But it can also back up other files and folders if you simply add them to a Windows Library. Likewise, you can exclude files and folders from File History by removing them from a library.

File History also automatically backs up four standard Windows user folders: Desktop, Favorites, Contacts, and anything stored in your local OneDrive folder (which I'll come back to in the next section).

To get up to speed quickly on File History's configuration, customization, and use, see the following:

- "Understanding Windows 8's File History" – July 11, 2013, Top Story
- "Windows 8: File History explained" – TechNet article
- "Set up a drive for File History" – MS how-to
- "Customize File History's backups with ease" – Oct. 9, 2014, LangaList Plus (paid content).

Keep in mind that File History makes incremental backups every hour, by default. But you can have it run as often as every 10 minutes. As a result, File History can consume a lot of disk space. The advanced settings (Figure 2) let you control how often File History runs and how long it should save backup files. For more on this, see the July 11, 2013, Top Story listed above and the Nov. 6, 2014, LangaList Plus column, "How to shrink huge File History backups."

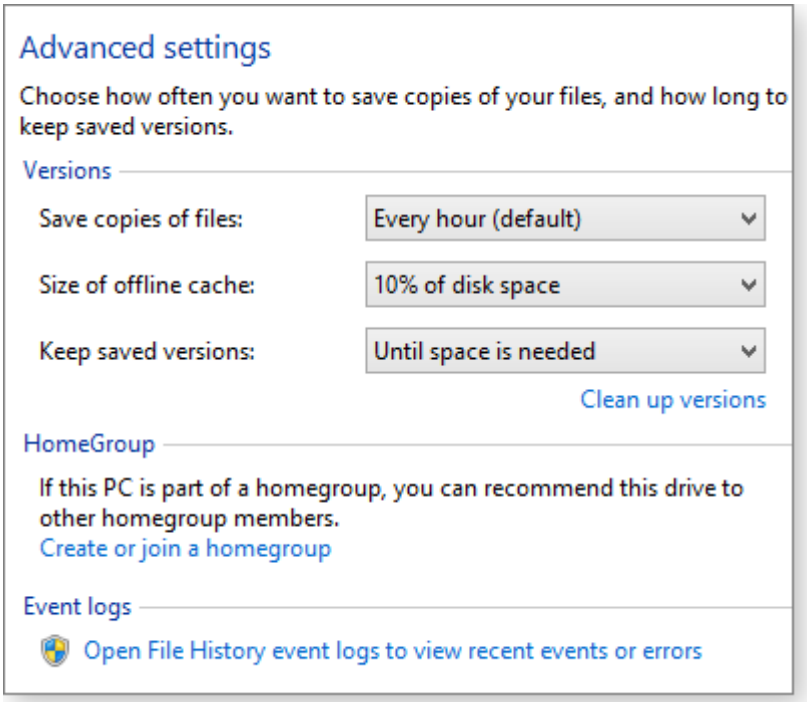

Figure 2. File History's advanced settings let you configure the frequency of backups, how much disk space they consume, and how long they're kept.

(A related article discusses how to work around a rare but annoying bug that can cause File History to back up every file, every time. See the Aug. 15, 2013, LangaList Plus column, "Solving File History's 'excessive saves' bug" [paid content].)

File History can also have connection issues with multiple external drives. If you routinely connect and disconnect various external drives, check out the March 6, 2014, LangaList Plus item, "How to make File History retain drive IDs." Your hard drive's sleep and suspend cycles can also interfere with File History's ability to make backups. See the Nov. 28, 2013, LangaList Plus, "A warning regarding Win8's File History."

With File History properly configured, Win8 will make reliable and automatic local backups of whatever files you've set it to maintain.

How OneDrive adds another layer of data security

All Windows 8 users should be familiar with Microsoft's OneDrive online service. Again, it's built into the operating system and automatically gives Win8 users 15GB of free, cloud-based storage. (Additional storage is surprisingly inexpensive; see MS info.)

But OneDrive does more than store copies of your data files. By default, Win8 automatically backs up seven types of personalization/customization settings to your associated OneDrive account: Start screen layout, color scheme, theme and background, language preference, browser history, browser favorites, and the settings for any apps you obtained from the Windows Store. (For more on this, see the Dec. 11, 2014, LangaList column, "Controlling Win8's auto-synching of settings.")

Anything you or your software saves or adds to OneDrive is automatically stored in the cloud on Microsoft servers. But OneDrive does much more — though Microsoft does a terrible job of explaining those capabilities.

For example, the local OneDrive folder on your **C:** drive normally stores only snippets and partial copies of any files you're working on; the full copies reside in the cloud. But OneDrive also offers a **Make**

available offline option. Any files or folders to which you apply the option are fully available for offline access; OneDrive automatically stores a second complete copy of the file or folder on your hard drive.

That's the key to Win8's outstanding data redundancy. If you store your important files and folders in OneDrive and then use the **Make available offline** option, OneDrive makes two complete copies. When combined with File History, you end up with:

- A live copy in the OneDrive folder on your hard drive
- A backup copy stored in the cloud on the OneDrive servers
- A local backup saved by File History on a second (typically external) drive.

That's about as bulletproof and automatic as a backup system gets!

Moreover, because File History makes frequent, incremental backups, the **Make available offline** option provides a form of ***versioning*** for your OneDrive-based files. Your local OneDrive folder and the OneDrive servers will always contain the most recent copy of any included file, and File History will contain as many previous iterations of the file as you've configured it to capture.

The **Make available offline** option is easy to implement: in File Manager, open your OneDrive folder and right-click any included file or folder. Then select **Make available offline,** as shown in Figure 3. It's that simple.

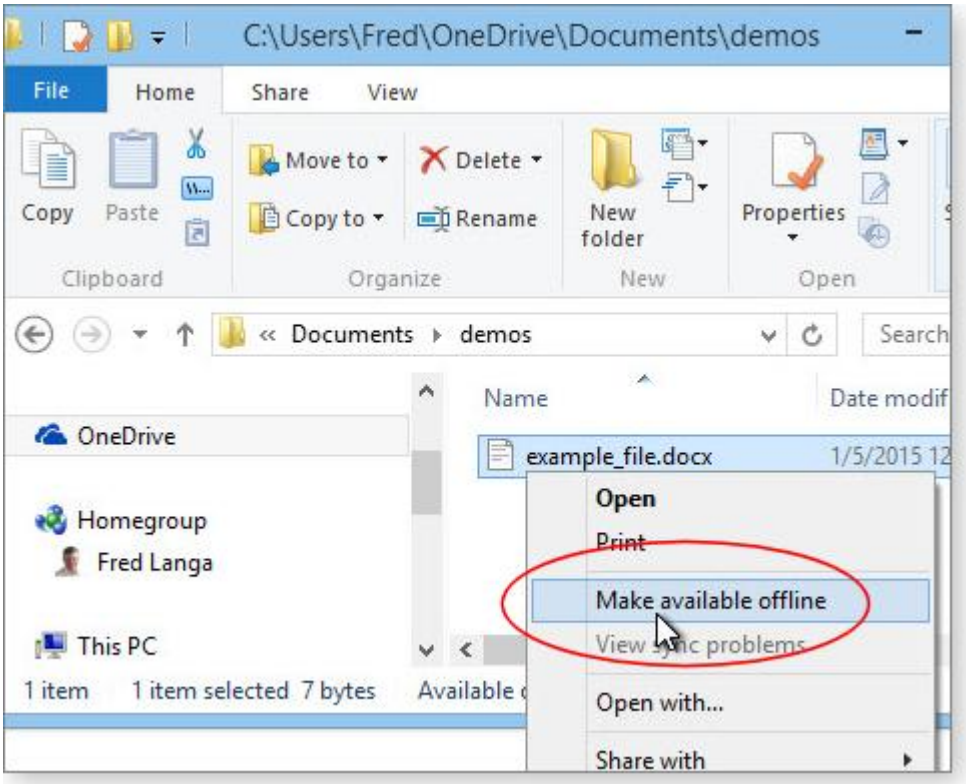

Figure 3. Selecting *Make available offline* gives any OneDrive file or folder three-way redundancy: hard drive, cloud, and File History.

For me, the "Make available offline" — combined with OneDrive in the cloud and local File History — is the best feature of the Win8 backup system. It should be enough to protect your data against almost any imaginable form of loss.

OneDrive is generally easy to access and use; but if you'd like more information, see these Microsoft sources:

- "Getting started with OneDrive" – tutorial
- OneDrive FAQ
- OneDrive support.

Note: There's a potential OneDrive issue that Microsoft does not cover well. The service is linked to your Microsoft account, which you also use when signing in to Win8 systems. But Win8 also allows for other types of sign-ins — seven in all — and not all of them allow for automatic access to OneDrive.

If you have trouble accessing your OneDrive account — or for tips on how to prevent access trouble in the first place — see the Jan. 8 LangaList Plus column, "Taming Win8's seven-way sign-in hassles."

Security Note: It's always wise to encrypt your most sensitive folders or files to prevent snoops from being able to access them — especially if the data will be transmitted over the Internet or stored in a cloud-based server. I use 7-Zip (free; site) to apply 256-AES encryption to sensitive files and folders stored in my local OneDrive folder. The encrypted files are then automatically replicated to the cloud and to my File History backups.

A refresher on Win8 OS and software restorations

File History and OneDrive deal mostly with user files and data. But as mentioned above, Win8 provides separate mechanisms for backing up and restoring operating-system files and installed software.

Refresh: Windows 8's 'Refresh your PC without affecting your files' feature returns system files to their original condition while leaving the users' accounts, data, passwords, and personal files largely untouched. But there are limitations. For example, Refresh removes any non-native Windows 8 (typically, desktop) apps that you've installed. For full information, see the Aug. 15, 2013, Top Story, "A 'no-reformat reinstall' for Windows 8."

Reset: If a refresh doesn't work. Win8's 'Remove everything and reinstall' option wipes out your existing setup and rolls Windows back to its initial, out-of-the-box state. For details on this process, see the Sept. 12, 2013, Top Story, "A clean-slate reinstall for Windows 8."

Microsoft doesn't stress this, but I will: **Reset is designed to work with File History.** After a system reset, File History can automatically repopulate your Documents, Music, Pictures, Videos, Desktop, Favorites, Contacts, and any other folders or files you've added to File History — such as OneDrive items you've made available offline. Depending on how your system is set up, the post-Reset file-restoration process might be fully automatic, or it might require a few clicks to get started. (See the Win8 how-to, "Restore files or folders using File History.") Either way, it's an almost effortless way to get back all your user files and data after an operating system reset.

Customized system recovery images: Win8's built-in **Recimg.exe** tool (Recimg, for short) is a command-line option that creates custom system images (see Figure 4). When needed, custom images can return Win8 to a user's specific configuration — including all applications installed when the custom image was made (not just native Win8 apps). For detailed instructions, see the Oct. 10, 2013, Top Story, "Creating customized recovery images for Win8."

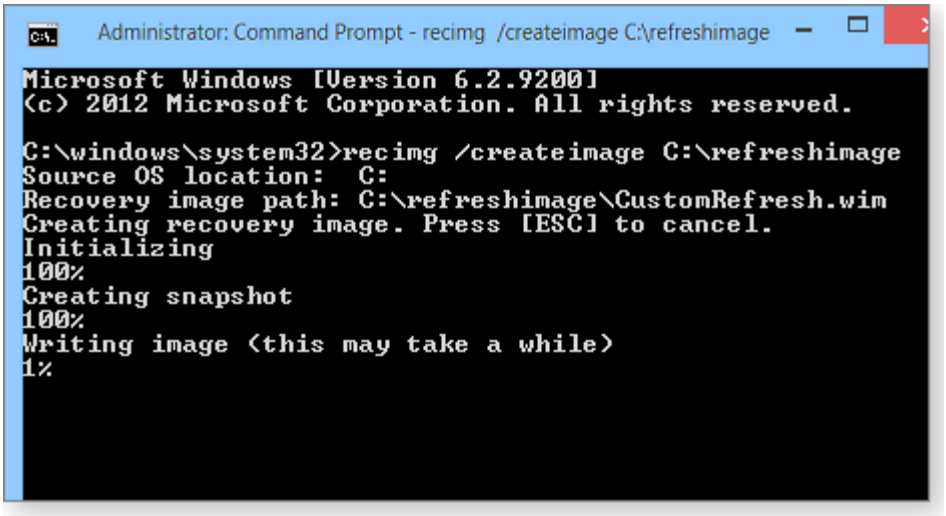

Figure 4. A typical *Recimg* progress screen

Once Windows is fully restored from a custom system image, use File History to restore the latest copies of your files.

Note: If you use encryption products such as TrueCrypt, VeraCrypt, or Boxcryptor that create "containers" with assigned drive letters, you can't make custom system images. If you try it, **Recimg** will simply fail with a generic error message. For more information and a workaround, see the Dec. 11, 2014, LangaList Plus, "Why VeraCrypt won't work with Windows 8."

Make sure you can access your backups

Obviously, backups are worthless if you can't get to them. You should be able to access your backups regardless of the circumstances — even if Windows won't run or your PC won't boot from its hard drive. Be sure you have a working bootable emergency-repair disk or drive. These articles can help:

- "Emergency repair disks for Windows: Part 1" – April 10, 2014, Top Story.
- "Emergency repair disks for Windows: Part 2" – April 17, 2014, Top Story

If you have trouble booting your system from the emergency disc, see:

- "How to solve UEFI boot and startup problems" – Dec. 11, 2014, Top Story
- "Emergency access to your PC's UEFI [boot] settings"– in this issue's LangaList Plus section (paid content).

Third-party backup/restore alternatives

Nothing's perfect. Although Win8's backup/restore system works well in most circumstances, it might not be a good fit for your particular configuration. Or you might simply not want to trust your data to the cloud.

If that's the case, there are numerous third-party backup tools that can produce traditional backups and images of your Win8 system. Some of the more popular products include:

- Macrium Reflect – free and paid (with free trial) versions
- Paragon Backup & Recovery – 30-day demo and paid versions
- Acronis True Image – paid with 30-day free trial (site)
- EaseUS Todo Backup – free and paid versions.

For some Windows 8 setups, an automated cloud-based backup service might be more suitable. See Lincoln Spector's Nov. 20, 2014, Best Practices story, "Cloud data protection: Synching versus backup" [paid content]. You can find more alternatives by doing a Web search for "windows 8.1 local backup."

***Win8 backups: Significantly different but arguably better*.** Microsoft did a poor job of documenting backup and recovery in Win8, and getting used to the process does take some effort. But it's well worth taking some time to understand and implement Win8's built-in backup-and-restore tools.

Once configured, Win8's backup system offers automated, redundant, near-real-time data security that most traditional backups simply can't match.

Try the Windows 8 way — you'll probably never go back!

Last year I joined a group for procrastinators. We haven't met yet!

SSD Drives: Good For the Long Haul?

Category: Hard-Drives From "askbobrankin.com".

Solid State Drive (SSD) technology has been taking over the mass storage market rapidly. But there's always been uncertainty about the useful lifespan of a solid state drive, as compared to a traditional magnetic drive. Will your SSD conk out suddenly, or will it last for years? Read on... 51

SSD Drives Keep Going and Going

SSD capacities keep rising, prices keep falling, and SSDs show up in everything from phones to desktop gaming PCs, high-end workstations, servers, and any place where magnetic hard drives have dominated for decades. It's easy to understand the enthusiasm for SSDs.

An SSD drive is much faster than a magnetic drive; that means faster boot times and more responsiveness in applications, particularly when dealing with large data files. With no moving parts, SSDs are silent and less subject to mechanical failures.

But rumors persist that SSDs won't last as long as mag drives. Manufacturers provide warranties ranging between 3 and 5 years, but that doesn't satisfy the skeptical. A warranty won't replace your irreplaceable photos, videos, music collection, and so on. Everyone wants to know,

“How long will an SSD last?”

The uber-geeks at Tech Report decided to answer that question once and for all by writing 100 MB blocks of data to six consumer-grade SSDs until all of the drives die. The torture test started in August, 2013; as of June, 2014, only half of the drives have given up the ghost. It’s obvious at this point that if your purchase a SSD today, it will probably outlive you.

The six drives tested are nothing special, just off-the-shelf consumer SSDs that you can pick up at Best Buy, Tiger Direct, or even Walmart. The line-up includes : the Corsair Neutron GTX 240GB, Intel 335 Series 240GB, Samsung 840 Series 250GB, Samsung 840 Pro 256GB, and two Kingston HyperX 3K 240GB.

Megabyte, Gigabyte, Terabyte, Petabyte...

Each of the drives is warranted to last for at least 200 terabytes of data writes. That’s a lot more than the typical home or small business user will write in 3 to 5 years. Usually, manufacturers tend to over-promise on such things, but these SSD drives are surprising everyone.

In addition to standard magnetic drives and solid state drives, there's another option: The Solid State HYBRID Drive, which combines the best features of both styles. See my related article: What is a Solid-State Hybrid Hard Drive?

The first fatality, a Kingston HyperX 3K, wrote 728 terabytes before giving up the ghost. The second SSD to die was the Intel 335, at 750 TB. The Samsung 840 Series gasped its last at 900 TB.

Three SSDs have made it past the 1 Petabyte milestone. A petabyte is 1,000 Terabytes, a nearly incomprehensible number normally found only in NSA or NASA IT projects. The first three seasons of the HBO hit, “Game of Thrones,” in 1080p MP4 format, occupies 9,285,418,071 bytes (9.3 GB). One petabyte equals about 107,695 copies of that data set.

It’s noteworthy that NONE of the SSDs failed until they were 3.5 times past the manufacturers’ data-writing warranty, which is about 9-15 years’ worth of normal home use.

So if anyone suggests that SSDs don’t last as long as magnetic drives, point them to this article. If you really want to bury them in excruciating details about the Tech Report testing methodology, SSD data storage techniques, and other geekiness, point them to the still-running thread, SSD Endurance Test.

Bottom line, any of the latest crop of consumer SSD drives seems likely to outlive your computer, and will probably last as long or longer than a magnetic drive. But don't use that as an excuse to avoid doing regular backups. See my Backup Articles to learn more about that.

From Your Editor!

“That’s all folks!”