August, 2018
Volume 13, Issue 8

Want to keep your data? Back it up!

From the desk of Thomas F. Duffy, MS-ISAC Chair

We all know it happens – computers crash, malware infects them, or somebody downloads that cool, new program that crashes everything! While there are many tips and tricks of great value for preventing your devices and data from being compromised, it is important to also have a backup of your information in case something goes wrong!

Backups are copies of key information or data that are stored separately from your device. By storing these separately, you can restore your data or device using these backups and get right back to full working order. With threats of Ransomware, which encrypts and renders your personal files inaccessible, this is a real concern. Below we will explore some key concepts on creating and will provide resources that assist you in making decisions on how to best create this essential type of redundancy in your life.

Choosing what to backup

When thinking about a backup system the first thing to decide is how much you want to backup. Are you okay storing key documents, pictures, and files or do you want your full system backed-up? If you're concerned about rebuilding a full system, and a having all the license information to make it functional, then you probably want a more complete backup option. If you just want to protect important files, then a system where you choose what to save would work well.

How can you create a backup of just key files?

If you are looking to store copies of your important files, you can copy them to your preferred method of backup periodically. This is accomplished by selecting the folders or files you want to backup, and copying them to the storage device or media. This is made especially easy if you make a habit of organizing your important files into just a few folders. This is a very simple and easy approach, and guarantees that your tax documents, digital receipts, pictures, and other important records remain available.

How can you create a complete backup of your device's data?

If you are looking to create a more comprehensive backup, your devices likely have utilities built in that allow for easy creation of backups. These may allow you to set a complete copy of your device's data aside that would allow you to restore it to full working order following an infection or issue. Seek out guidance or tips from your device's vendor to determine what utilities are available to you for creating backups. The Stay Safe Online guide linked below has links to top vendors backup guides that can assist you through the process.

Choosing where to store your backed-up data

Regardless of what you want to save, one of the key ways to keep your backed-up data safe, is to disconnect the storage media after you make the backup. This is important in the event that you are infected with malware, as you do not want the copies of data to also be infected. (Ransomware does look for backups to infect!) This also helps in case your computing device or where you store it is lost, stolen, or physically destroyed. Keeping a separate backup on a different physical storage device, or in the cloud, is a way to better secure your data from this type of problem.

Cloud services for storing backups can be a convenient solution, though they may come at a cost and some individuals may not like the fact that they will not have a copy in hand on physical storage media. Having the backup outside your immediate possession can be helpful if you are concerned about a physical problem, such as loss or damage. Some of these services save multiple versions of your backup, which better secures against infected files corrupting the cloud backup.	***External hard drives or removable media (DVDs, USB drives, etc.)*** are the other most common option. You simply need to copy the data you want to save to the external hard drive or media. Consider keeping the external drive disconnected from your devices while not making backups, as this insures against malware getting on the backup copy.

How often should you back up files and systems?

The frequency with which you back up your data or systems is an important component of this process. Consider making your backups on a weekly basis, with a minimum frequency of monthly backups.

In conclusion, spend time considering how vital the data on each of your devices is. Then consider the best type of backup strategy for your needs and base a timeline of how frequently you make the copies off those needs as well. By adding this simple process to your safe computing habits, you can build in more reliability and recoverability. If you are ever the victim of a malware infection or cyber attack, you will surely be glad you took the time to make backups!

Suggested resources:

https://staysafeonline.org/stay-safe-online/online-safety-basics/back-it-up/
https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™