

In our [“What’s Possible with Modern Data Recovery”](#) post, we learned about how professional data recovery experts can (in most cases), recover lost data from a damaged or compromised hard drive or solid state cell by using a variety of methods. While these specially-trained technicians have an excellent rescue rate once they receive a failed drive, there are a number of steps you can take immediately after a failure that will help increase your chances of a full recovery.

Any data storage device can fail—whether it is from normal wear, fire, moisture, electronic interference, or physical damage—any data that is not properly backed up to a separate device (or the cloud), is at risk. When data loss happens to you, your next steps can be crucial—and can mean the difference between recovery and permanent data loss.

First Steps

If your rotational hard drive is making clicking, grinding or whirring sounds, shut down your computer immediately. These sounds could be the read/write heads hitting or scraping the hard disk platters—and severe, or complete data loss could result—so keep these points in mind:

- If possible, back up your important data immediately.
- Do not use data recovery software if the hard drive makes scraping, tapping, clicking or humming sounds—these are signs of internal physical damage, and intensely scanning the drive may cause irreparable damage
- Avoid powering-up a device that has obvious physical damage or is making unusual sounds.
- Do not attempt recovery on severely traumatized drives (wet, fire damaged, dropped, etc.). If water damaged, seal the drive in a plastic baggie with a moistened paper towel inside to maintain the humidity.

If your data is critical, (and whose isn’t) be sure to choose a reputable recovery firm that can properly recover data from mechanically failed or physically damaged drives. Avoid “home remedies” you may have read about on the web such as placing a non-spinning hard drive in a freezer or hitting a drive on its side. These unproven methods can actually harm the device further, and could possibly render the drive useless.

Best Practices

There are a number of best practices to help avoid data loss:

- Use up-to-date hardware and software utilities for data security, such as firewalls and virus protection, and make sure to have a verified backup of all your data before installing or upgrading the operating system
- Scan all incoming data; such as emails, websites and downloads for viruses and malware.
- Connect computers and data servers to an uninterruptible power supply (UPS) to protect against power surges or outages.
- Avoid static discharge when touching or handling any storage media, especially in excessively dry environments.

Create a Backup Plan

Of course, backing up your data regularly is probably the best way to avoid data loss in the first place. Invest in a redundant backup system like a direct-attached drive exclusively for backup, like [My Book Duo](#), and an additional network attached storage (NAS) system, like [My Cloud PR2100](#), or cloud-based backup service. Schedule a daily or weekly backup to an external source—most NAS systems have pre-installed software that can help you automate this process, and periodically test the backups by restoring a few files and verifying the data.

Choosing a backup device with dual drives in a RAID 1 configuration creates a duplicate copy of your data on the second drive. In the event one drive fails, a complete copy can be restored from the second drive. Combine this with a backup of your files on a separate external storage device—giving you good protection against data loss. Of course, a RAID 1 configuration may not be enough—you should always have a separate backup device (or cloud service) in case your RAID 1 device fails on a device level.

In the upcoming posts, we will explore in-depth, the methods used to recover data from all types of devices, including hard drives, solid state drives, tablets, smartphones, RAID-configured arrays, and more.