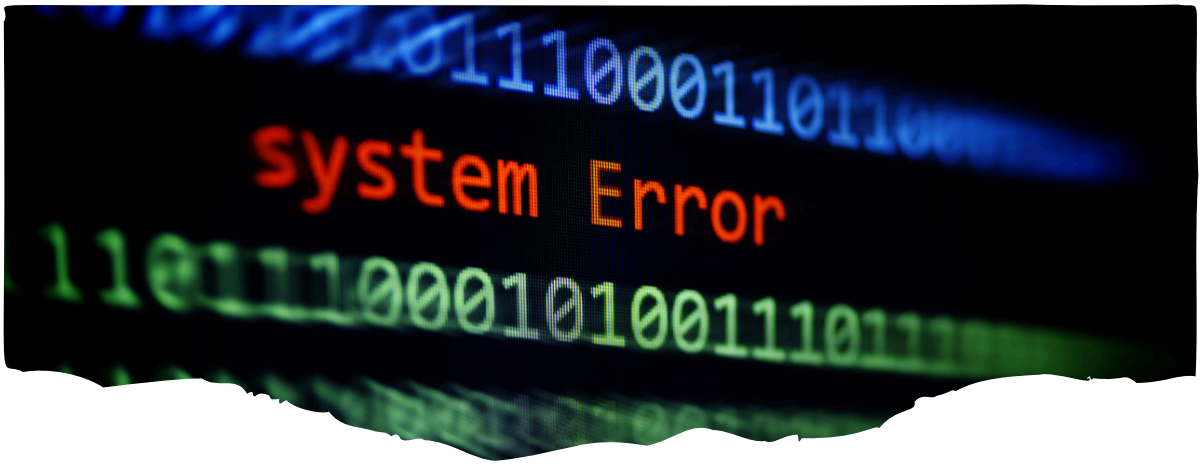


WHY BACKUPS ARE ESSENTIAL

Contributed by the Technology Advisory Committee

Many people store important data on devices like laptops, desktops, external drives, or USB sticks. However, failingto secure or back up this data increases the risk of breaches, theftor permanent loss. Various threats highlight the need for backups. Malwarecan infiltrate your device, modifying or stealing files, while ransomware may lock your data until a ransom is paid, possibly rendering it permanently inaccessible. Opportunistic criminals may steal your device, resulting in data loss if it's not backed up.

Targeted attacks can exposesensitive information for identity theft,and natural disasters like fires or floods can destroy storage devices.
Backing up your data is quick and can often be automated, requiringminimal effort to prevent significant stress later.

What Is a Backup?

A backup is a secure copy of your data stored in a different location, either online in the cloud or offline on removable media. If you lose access to original data, a backup allows you to restore it and avoid costly losses. Backups can be comprehensive, capturing all files and system data, or selective, targeting essential documents, photos and videos. Anything that would cause inconvenience if lost should be backed up.

How to Back Up Your Data

Cloud Storage for Online Backups

Cloud services, including, but not limited to, iCloud, Google Drive, and OneDrive offer secure remote storage. These services typically provide limitedfree space, sufficientfor essential files.Cloud backups are automated, ensuring data remains current. They also allow access from any internet-connected device, valuable if your primary device is lost or damaged. However, cloud storage requires a reliable internet connection, and large backups may incur additional costs.

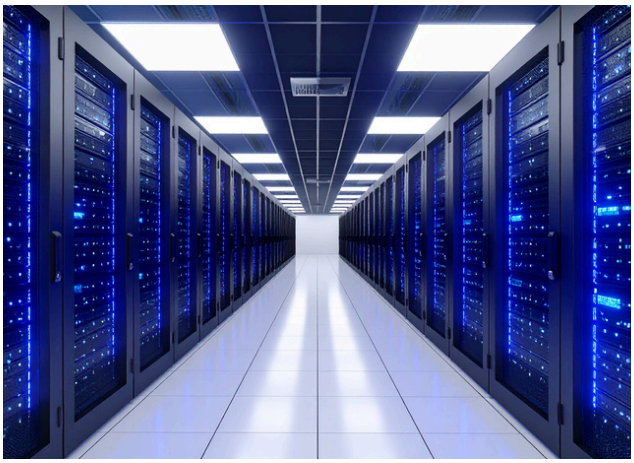
Removable Media for Offline Backups
Offline backups can be made with external media. These devices don't require internet access for transfers and involve a one-time investment rather than ongoing cloud service fees. To protect offline backups, disconnect storage devices when not in use to avoid malware infections. Manual file copying or automated backup systems can make the process more convenient.

Implementing Your Backup
The United States Computer Emergency Readiness Team (US-CERT) recommends the 3-2-1 backup rule:
3 Keep three copies of important files – one primary and two backups.
2 Store backups on two different media types (e.g., an external hard drive and cloud storage).
1 Keep one copy off site (e.g., in the cloud) to safeguard against local disasters.

Protecting Your Backup
Security is crucial for backups, particularly for cloud-based solutions. Protect cloud accounts with strong passwords and enable two-factor authentication (2FA) to prevent unauthorized access. (Refer to this previous article for detailed information about two-factor authentication.)

Maintaining both online and offline backups offers added assurance that your data remains accessible. Limiting physical access to your data provides another layer of security.

Restoring and Verifying Backups
Regularly verify your backups contain recent and essential data. Storing irreplaceable files in both cloud and offline locations ensures they're always accessible. Features like the recycle bin and file history help you recover accidentally deleted files without restoring the entire backup.
By adopting these strategies, you can protect your digital assets from unforeseen threats and recover valuable data when needed.



Sources:

University of Wisconsin-Madison Libraries

Cybersecurity and Infrastructure Security Agency (CISA)

United States Computer Emergency Readiness Team (US-CERT)

National Cyber Security Centre (UK)

American Association of Retired Persons (AARP)

National Cybersecurity Alliance