BACKING UP SAFELY

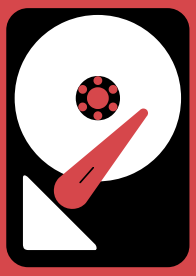
Backups can be a life saver. If your device is ever lost, stolen, corrupted, or compromised you can quickly revert to a backup. However, depending on your backup methodology you can expose yourself to additional risk by opening your backups to compromise.

Here are two options for backing up data:

OPTION 1

Remote backups built into your OS such as Apple iCloud or Microsoft OneDrive are often the easiest way to back up your computer and data; however, they can also be the most vulnerable. Consider the recent iCloud incident where private celebrity images were stolen from Apple iCloud.

OPTION 2



If the data is sensitive in nature, all backups should be stored fully encrypted. For local backups, an encrypted external hard drive can be used specifically for storing backups. For remote backups, data should be encrypted before uploading to third party servers.

BEST PRACTICES

- Fully encrypt any backups with a strong passphrase.
- Store sensitive backups on an external drive that only you can access.
- Encrypt data locally before storing it remotely.
- Test your backup system periodically to ensure it works.
- Where possible, backup your full system configuration in addition to all of your data.
- Windows System Restore is often not sufficient for backup purposes as malware often attempts to wipe it and if the hard drive fails the backups are lost.

SECURITY INNOVATION