CMSGu2017-03

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on devising a personal backup plan

CERT-MU

National Computer Board
Mauritius

September 2017

Issue No. 3

Version 1.0

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to give users a guidance on what kind of backup plan they should adopt to protect their data against loss or theft.

1.2 Audience

The targeted audience for this document includes everyone who uses electronic devices such as computers, laptops, smart phones and tablets.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on data loss and the need to backup information.

Section 3 explains how to protect against data loss through regular backups.

Section 4 discusses different types of backup plans.

Section 5 shows how to back up and restore files using Windows 10.

Section 6 concludes the document.

Section 7 comprises a list of references that have been used in this document.

2.0 Background

The rising use of electronic devices such as laptops, tablets, smart phones and other personal electronic device have made these devices become a target of choice for thieves. As these devices make it easier to store and access information for personal and professional use, they can also put your data at risk. Theft is a significant threat to users of these devices, especially when using them to access your personal information, bank accounts, or work information.

The cost of a stolen tablet, laptop, or other small electronic device is not solely its replacement cost, but also the cost of peripherals and accessories, the installed software, and the cost of any information that is compromised from that device.

An even greater cost is the potential exposure and liability that may result from any compromised confidential corporate and client information.

Criminals are increasingly becoming more innovative and inventive in finding ways to steal valuable information from mobile devices and laptops that do not have appropriate security. So we have to be aware, secure, and more importantly, prepared with our personal backup plan.

3.0 Protecting yourself against data loss through regular backups

The only way to protect yourself against valuable data loss is through regular backups. Ideally, important files should be backed up at minimum once a week, or every day, depending on how critical they are to you. This can be done manually, automatically, or using combination of the two methods.

When it comes to backups, just like security, you want to find a balance of being thorough but efficient. We have all heard disastrous stories of losing homework due to the blue screen of death or a misplaced cell phone that tragically stored the only copy of family photos. In addition, you could fall victim to ransomware or another malicious attack that leaves you with no choice but to reimage your computer. It never hurts to consider your backup strategy and come up with a plan that leaves you feeling safe and secure. Here are some tips to get you started.

- Data loss happens all the time, but it is entirely preventable. You just need to create a backup plan.
- Your critical data should never reside in a single place.
- The ideal backup strategy will typically include both an online backup service (e.g., Dropbox, Box, OneDrive, Google Drive, CrashPlan, iCloud) and an offline backup utility (e.g., external hard drives, flash drives) to ensure your data is secure no matter what happens to your mobile device or computer.
- Running consistent, automatic backups is a straightforward process that will take little time to set up and will require even less to maintain.
- Backups can be configured to run in real time when files on your computer are changed.
- Routinely test your backup solution to ensure you can recover your data in the event that you do actually need to restore from a backup.

4.0 Types of backup plans

There are many ways to back up your data, from using an external drive to backing up those files on a remote server over the Internet. Here are the strengths and weaknesses of each:

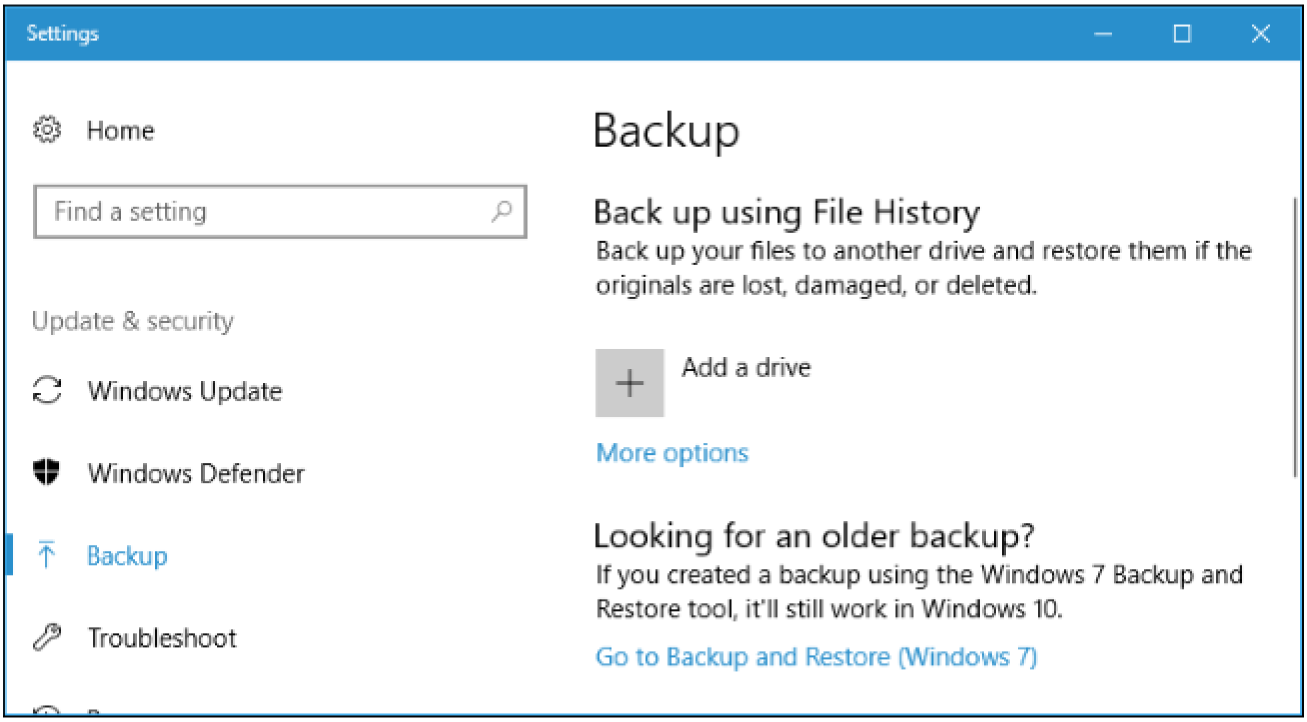
4.1 Back Up to an External Drive

If you have an external USB hard drive, you can just back up to that drive using your computer's built-in backup features.

- On Windows 10 and 8, **use File History**.
- On Windows 7, **use Windows Backup**.
- On Macs, **use Time Machine**. Occasionally connect the drive to the computer and use the backup tool, or leave it plugged in whenever your home and it'll back up automatically.

Pros: Backing up is cheap and fast.

Cons: If your house gets robbed or catches on fire, your backup can be lost along with your computer.



Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Looking for an older backup?

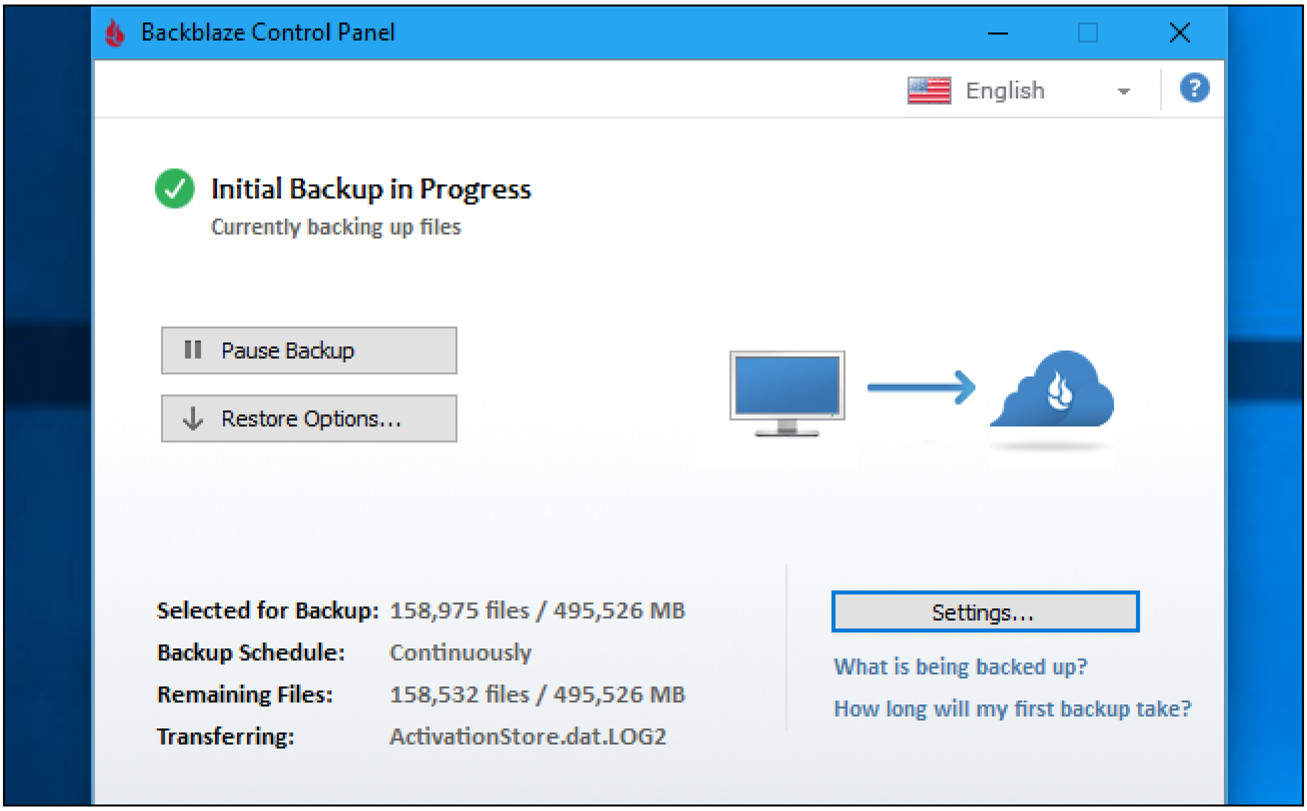
If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

4.2 Back Up Over the Internet

If you want to ensure your files stay safe, you can back them up to the internet with a service such as **BackBlaze**. BackBlaze is the well-known online backup service. There are also other vendors such as **Carbonite** and **MozyHome** that can be used for backup. For a low monthly fee, these programs run in the background on your PC or Mac, automatically backing up your files to the service's web storage. If you ever lose those files and need them again, you can restore them.

Pros: Online backup protects you against any type of data loss–hard drive failure, theft, natural disasters, and everything in between.

Cons: These services usually cost money, and the initial backup can take much longer than it would on an external drive–especially if you have a lot of files.



Initial Backup in Progress

Currently backing up files

Selected for Backup: 158,975 files / 495,526 MB

Backup Schedule: Continuously

Remaining Files: 158,532 files / 495,526 MB

Transferring: ActivationStore.dat.LOG2

What is being backed up?

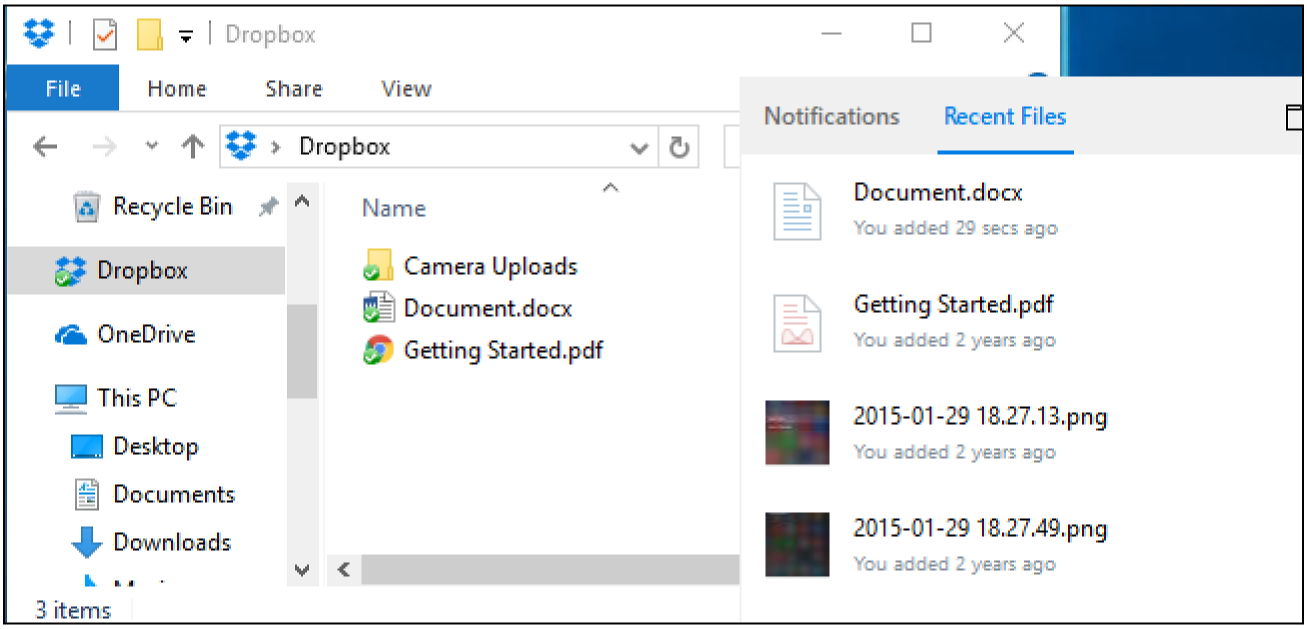
How long will my first backup take?

4.3 Use a Cloud Storage Service

Rather than just storing your files on your computer's hard drive, you can store them on a service such as **Dropbox**, **Google Drive**, **Microsoft OneDrive**, or a similar cloud storage service. They will then automatically sync to your online account and to your other PCs. If your hard drive fails, you will still have the copies of the files stored online and on your other computers.

Pros: This method is easy, fast, and in many cases, free, and since it's online, it protects you against all types of data loss.

Cons: Most cloud services only offer a few gigabytes of space for free, so this only works if you have a small number of files you want to back up, or if you're willing to pay for extra storage. Depending on the files you want to back up, this method can either be simpler or more complicated than a straight-up backup program.



4.4 Which method to use?

While backup programs like **BackBlaze** and cloud storage services like Dropbox are both online backups, they work in fundamentally different ways. Dropbox is designed to sync your files between PCs, while BackBlaze and similar services are designed to backup large amounts of files. BackBlaze will keep multiple copies of different versions of your files, so you can restore the file exactly as it was from many points in its history. And, while services like

Dropbox are free for small amounts of space, BackBlaze’s low price is for as big a backup as you want. Depending on how much data you have, one could be cheaper than the other. BackBlaze and Carbonite do have one big limitation. If you delete a file on your computer, it will be deleted from your online backups after 30 days. You cannot recover a deleted file or the previous version of a file after this 30 day period.

4.5 Using multiple methods

Ideally backups should be performed both offsite and onsite. Onsite backups means backups stored at the same physical location as you. So, if you back up to an external hard drive and store that at home with your home PC, that’s an onsite backup. Offsite backups are stored at a different location. So, if you back up to an online server, like BackBlaze or Dropbox, that’s an offsite backup.

Onsite backups are faster and easier, and should be your first line of defense against data loss. If you lose files, you can quickly restore them from an external drive. But you should not rely on onsite backups alone. If your home burns down or all the hardware in it is stolen by thieves, you will lose all your files.

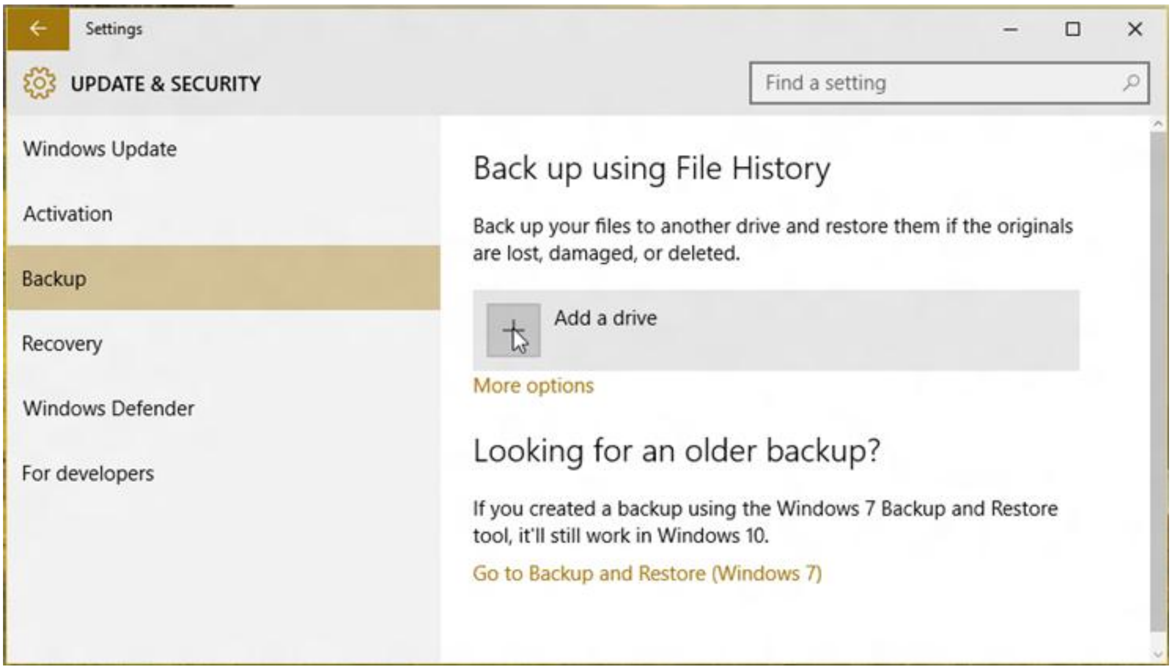
Offsite backups do not have to be a server on the Internet, either, and you don’t have to pay a monthly subscription for one. You could back up your files to a hard drive and store it at your office, at a friend’s house, or in a bank vault, for example. It will be a bit more inconvenient, but that’s technically an offsite backup.

Similarly, you could also store your files in Dropbox, Google Drive, or OneDrive and performing regular backups to an external drive. Or you could use BackBlaze to back up online and Windows File History to create a local backup. There are a lot of ways to use these services together, you just have to ensure you have a solid backup strategy, with onsite **and** offsite backups, so you have a better protection against losing your personal information.

5.0 Backing up and restoring your files using Windows 10

5.1 Setting up your backup

Select the **Start** button, select **Settings** > **Update & security** > **Backup** > **Add a drive**, and then choose an external drive or network location for your backups.



Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

All set. Every hour, we'll back up everything in your user folder (C:\Users\username). To change which files get backed up or how often backups happen, go to **More options**.

5.2 Restoring your files

If you're missing an important file or folder, here's how to get it back:

1. Type **Restore files** in the search box on the taskbar, and then select **Restore your files with File History**.
2. Look for the file you need, then use the arrows to see all its versions.
3. When you find the version you want, select **Restore** to save it in its original location. To save it in a different place, press and hold (or right-click) **Restore**, select **Restore to**, and then choose a new location.

6.0 Conclusion

Computer loss, theft, natural disaster, and accidental deletion, are just some of the ways that you can lose your personal data. The only way to prepare for the unexpected is to have a good backup strategy in place. There are many different ways to backup your computers, and using multiple forms of backup will minimize the risk of ever losing your valuable files.

7.0 References

- **https://www.it.ucla.edu**
- **https://er.educause.edu**
- **https://www.howtogeek.com**
- **https://www.backblaze.com**