Part 6

Backing Up and Recovery

IN THIS PART …

Find out about the different types of backups and how to use them.

Discover how to prepare a device before restoring from a backup.

Figure out how to restore from a backup.

Chapter 13

Backing Up

IN THIS CHAPTER

- **Discovering the importance of backing up**
- **Exploring different types of backups**
- **Encountering different ways to back up**

While backing up your data sounds like a simple concept — and it is — actually implementing an efficient and effective backup routine is a bit more complicated.

To properly back up, not only do you need to know about your backup options, but you need to think about many other details, such as the location of your backups, encryption, passwords, and boot disks. In this chapter, you find out about all those backup details and more.

Backing Up Is a Must

In the context of cybersecurity, *backing up* refers to creating an extra copy, or extra copies, of data (that may consist of data, programs, or other computer files) in case the original is damaged, lost, or destroyed.

Backing up is one of the most important defenses against the loss of data, and, eventually, it's likely to save you from serious aggravation, as nearly everyone, if not everyone, will, at some point, want to access data to which he or she no longer has access.

In fact, such scenarios occur on a regular basis. Sometimes, they're the result of human error, such as a person inadvertently deleting a file or misplacing a computer or storage device. Sometimes, they're the result of a technical failure, such as a hard drive dying or an electronic device

falling into water. And sometimes they're the result of a hostile action, such as a ransomware infection.

Sadly, many people believe that they back up all their data only to find out when something goes wrong that they do not have proper backups.

Don't let that happen to you. Be sure to back up on a regular basis — often enough that if you had to restore from a backup, you would not panic. In general, if you're in doubt as to whether or not you are backing up often enough, you aren't.

TIP Do not think of backups as being there for you if you ever lose data. Think of them being there for you *when* you lose data. At some point, essentially every person who uses electronic devices on a regular basis will lose data.

Looking at the Different Types of Backups

Backups can be categorized in many different ways. One important way of distinguishing various types of backups from one another is based on what is being backed up. The following sections look at the different types of backups based on that approach.

Full backups of systems

A *full system backup* is a backup of an entire system, including the operating system, programs/apps, settings, and data. The term applies whether the device being backed up is a smartphone or a massive server in a data center.

Technically speaking, a full system backup includes a backup of all drives attached to a system, not just those mounted inside of it — although if some drives are attached to the system only from time to time and are not needed for the primary use of the system, some might

exclude the contents of such drives from full system backups, especially if they're attached to other systems, or are backed up as part of the backup of other systems. For most home users, however, a full system backup means exactly what it sounds like: Backing up everything.

A full system backup is sometimes known as a *system image* because it essentially contains an image of the system as it existed at a particular point in time. If a device that you have an image of fails, you should be able to use the system image to re-create the entire system as it was at the time that the backup was made. When you use the rebuilt system, it should function exactly as the previous system did at the time of the backup.

TIP Full system backups are the form of backup that typically is fastest to restore an entire system from, but they take longer to create than other forms of backup. They also usually require more storage space.

One important caveat: Because a system backup includes settings, hardware drivers, and so on, restoring from a system image does not always work well if you restore to a different device than the one that was originally backed up. If you imaged a laptop that runs Windows 7 as its operating system, for example, and then acquired a newer device intended to run Windows 10, which has different hardware in it, a restored system image of the first device may not work well on the newer device. The reverse is even more likely to be true: If you keep an old computer in your closet "just in case" and that just-in-case situation turns into reality, your attempts to restore the image from a newer machine to the older machine may fail fully or in part.

TIP System images are sometimes referred to as *ghosts* (with ghost also being the verb for creating such images), especially among

techies. The name originates from one of the original disk cloning software packages for PCs.

Original system images

One special case of system images is the original system image, also known as a *factory image*.

Many modern computing devices, whether laptops, tablets, or smartphones, come equipped with a factory image that can be restored. This means that when you acquire the device, it comes with an image of the original configuration that you receive — including the operating system, all the original software, and all the default settings — stored in a hidden partition or other storage mechanism not normally accessible to users.

At any point in time, you can perform a *factory reset* and set your device to look identical to the way that it did when it was new. When you do so, the device restores from the hidden image.

WARNING Two important caveats:

- Some devices overwrite the factory reset image with new images in the event of certain operating system upgrades.
- If you factory reset a computer, all security updates installed since the factory image was originally created will not be present on the restored device. Be sure to update your system ASAP after restoring and before going online for any other purpose!

Later system images

Some systems also create periodic images that you can restore from without having to go back to the original factory settings. Windows 10, for example, has such capabilities built in.

WARNING Never restore from an image unless you know that any problems that developed and caused you to need to restore did so after that image was made.

Original installation media

Original installation media is for programs that you acquire and install after you purchased your device.

If software came on a DVD or CD, saving the physical media that it came on allows you to reinstall the software in case of a problem.

WARNING Keep in mind, however, that if any updates for the software were issued and installed subsequent to the original installation, you will need to redownload and reinstall the updates. Doing so may happen automatically upon reinstallation, or it may require manual effort.

Downloaded software

If you've acquired programs since you purchased your device, it's likely that some or all of them were delivered to you via digital download.

When software is delivered as a download, the downloader does not receive a physical copy. However, if you received software via a download, you can store a copy of the installation file that you downloaded on one or more of many different types of media, such as a thumb drive or a CD or DVD. Alternatively, you can store the copy on a hard drive, but be sure to back up that drive if it is part of your computer infrastructure.

Additionally, some stores that sell downloadable software maintain copies of the software for you in a *virtual locker* so that you can download it at a later date. Such "backups" are useful, but be sure that you know how long the store will maintain the product in your locker. Some people have had serious problems because they relied on such

“backups” only to find out that the software was not available to them at the time that they needed it.

TIP For music and video files, the vendor’s retention period is often theoretically forever, or at least as long as the material is available to purchase by others. For software, as new versions are released and old versions are *sunsetted* (the technical term for a software vendor phasing out and, ultimately, terminating support for an obsolete version of its software), the retention period may be far shorter.

Full backups of data

An alternative to performing a full backup of the entire system is to perform a full backup of the data on the system, but not of software and the operating system. (Configuration settings for both the operating system and various installed programs are often stored in data folders and included in such backups.) Performing a full data backup allows a user to restore all of his or her data in one shot if something goes wrong. Depending on the tool used to perform the backup, the user may be able to restore a subset of the data as well — for example, by choosing to restore only one particular file that he or she accidentally deleted.

REMEMBER Restoring from a full data backup will not restore applications. If a system has to be rebuilt entirely, recovering from full backups of data likely requires prior restorations to factory settings (or a later image of the computer) and reinstallation of all software. That is certainly more tedious than simply restoring from a system image. At the same time, it is also far more portable. The recovery can usually be done without any problems on many devices that vary quite a bit from the original device. Reduce the likelihood of your restored system suffering a security breach by updating the reinstalled software with the latest patches immediately after the relevant installations.

Incremental backups

Incremental backups are backups made after a full backup and that contain copies of only the portion of data (or, in the case of a system backup, the portion of the entire system) that has changed since the preceding backup (full or incremental) was run.

Incremental backups normally run much faster than full backups because, on most systems, the vast majority of data files do not change on a regular basis. For the same reason, incremental backups also use less storage space than do full backups.

To recover data, however, restoration must be done from the last full backup plus all the incremental backups performed since that last full backup.

TIP If you decide to use incremental backups, consider limiting the number of such backups that you create after a full backup. For example, if you did only one full backup on the first day of the calendar month and performed incremental backups on all subsequent days until the next month began, then if something went

wrong on the last day of the month, you would potentially need to restore from as many as 30 backups in order to recover your files.

Many people (and many businesses as well) choose to do full system backups on one of the days of the weekend and then do incremental backups during each other day of the week, thereby finding a happy medium between the efficiency gains during the backup process and the potential for a tedious recovering process.

Differential backups

Differential backups contain all the files that changed since the last full backup. (They are similar to the first in a series incremental backups run after a full backup.) A series of differential backups therefore requires more time to run and uses more storage space than incremental backups, but less than the same number of full backups. Recovering from differential backups can be faster and simpler than doing so from incremental backups because a restore needs to be done from only the last full backup and last differential backup.

If you decide to use differential backups, consider how many backups you should be making before making the next full backup. If the differential backup starts to grow quite large, there will not be much performance gains while making the backup, and any restoration will take far longer than if done from just a full backup.

Many people (and many businesses as well) choose to do full system backups on one of the days of the weekend, and then do differential backups during each other day of the week.

Mixed backups

Incremental and differential backups are made in conjunction with full backups, as shown in Table 13-1.

TABLE 13-1 A Comparison of Full, Incremental, and Differential Backups

	Full Backup	*Incremental Backup*	*Differential Backup*
Backup #1	All data	--	--
Backup #2	All data	Changes from Backup #1	Changes from Backup #1
Backup #3	All data	Changes from Backup #2	Changes from Backup #1

TIP Do not mix incremental and differential backups within the same backup scheme, as doing so can create complexity and lead to confusion and costly mistakes.

Continuous backups

Continuous backups refers to backups that run continuously. Every time that a change is made to data (or to a system and data), a backup of that change is made.

WARNING Continuous backups are great in case of a hard drive failure in the primary system — the backup is available and up-to-date — but do little in the case of a malware infection or data destruction, as the malware typically propagates to the backup as soon as it infects the primary system.

One exception are complex backup systems that log each backup action and have the ability to reverse them. These backups can undo problematic portions of backups to the point that they occurred.

TIP The process of continuously backing up is sometimes known as *syncing* (or *synchronizing*). You may see it described as such on your electronic devices or within various software packages.

Partial backups

Partial backups are backups of a portion of data. As opposed to full backups, partial backups do not back up all elements of data from a system. If a system were to be completely hosed, for example, you would have no way to fully recover all of its data contents from partial backups made earlier of that system.

Partial backups can be implemented in a full incremental-like model in which the first backup in a series includes all the elements that are part of the set included in the partial backup, and subsequent backups in the series include only items from that set that have changed.

Partial backups can also be implemented as always full-like — in which case, all elements of the set included in the partial backup are backed up each time, regardless of whether or not they have changed since the last backup.

REMEMBER Partial backups are not intended to be full backups in case of a malware attack or the like. They are useful, however, in other situations, such as one in which a particular set of files needs to be backed up separately due to the needs of a particular individual or group or due to the sensitivity of the material. For example, while the IT department may do full and incremental backups of all files on a shared network drive, the accountant who needs constant access to a particular set of spreadsheets stored on that drive — and would be unable to work if those files become inaccessible — may set up his own backup of just those files. He can use his backup if something goes wrong when he is on the road or working from home on the weekend, without the need to bother members of the technical support department at his firm to work unnecessarily on a Sunday.

Folder backups

Folder backups, are similar to partial backups in situations where the set of items being backed up is a particular folder. While backup tools can

facilitate folder backups, to the chagrin of many cybersecurity professionals and IT departments, many users perform such backups in an ad hoc fashion by manually making a copy of hard drive (or SSD) folders to USB drives at the end of each workday and consider such backups to be sufficient protection in case of problems.

Theoretically, of course, such backups work and can be used to recover from many problems. Reality dictates, however, that ad hoc backup procedures almost never result in proper backups: People forget on some days to back up or do not back up because they're hurried, neglect to back up some materials that they should have backed up, store the backups on insecure devices in insecure locations, or lose the devices on which the backups are stored — you get the idea!

If you want to be sure that you have proper backups when you need them — and, at some point, you are likely to need them — do not rely on ad hoc folder backups.

TIP Never back up a folder onto the same drive as the original folder resides. If the drive fails, you will lose both the primary source of data as well as the backup copy.

Drive backups

A *drive backup* is similar to a folder backup, but for situations where an entire drive is being backed up instead of only a folder. Ad hoc backups of drives do afford some protection, but rarely deliver sufficient protection against risks of losing data.

WARNING Never store the backup of a drive on the same drive as the one being backed up. If the drive fails, you will lose the primary source of data and the backup copy.

Virtual drive backups

One special case of drive backup is that in which a person or organization uses an encrypted virtual drive. For example, a user may store his or her files within a BitLocker drive on Windows. BitLocker is a utility built in to many version of Windows that allows users to create a *virtual drive* that appears as any other drive to the user when it is in use, but appears as one giant encrypted file when not in use. To access the drive, the user must unlock it, normally by entering a password.

Backing up such drives is often accomplished by simply including the encrypted file within the full, incremental, folder, or drive backup. As such, all contents of the encrypted drive are copied without being referred to by name and remain inaccessible to anyone who does not know how to open the encrypted drive. Many backups tools offer drive backups in addition to more structured forms of backup.

TIP Some software packages refer to the creation of an image of an entire disk as *cloning*.

While such a scheme protects the contents of the encrypted drive as they live in backups by using the same encryption as was used for the primary copies, note several caveats:

- **Even if one small change was made to a single file within the virtual drive, the entire encrypted file will be changed.** As such, a 1KB change could easily lead to an incremental backup having to back up an entire 1TB file.
- **The backup is useless for recovery unless someone knows how to unlock the encrypted drive.** While encryption may be a good defense mechanism against unauthorized parties snooping on sensitive files in the backup, it also means that the backup is not, on its own, fully usable for recovery. It is not hard to imagine problems developing as a result — for example, if someone attempting to utilize a backup several years after it was originally made forgets the access code, or if the person who created a backup is unavailable at the time that someone needs to restore from it.

- **As with all encrypted data, there is a risk that as computers become more powerful — and, especially, as quantum computing takes hold — today's encryption may not offer sufficient protection against brute force attacks.** While production systems will, no doubt, be upgraded with better encryption capabilities over time (as they already have been since the 56-bit encryption of the 1990s), backups that were made with old encryption technology and keys may become vulnerable to decryption by unauthorized parties. Hence, encryption may not forever protect your sensitive data contained in backups. You must store such backups in a secure location or destroy them when they are no longer needed.

Exclusions

Some files and folders do not need to be backed up unless you are imaging a disk (in which case the image must looks exactly like the disk).

Operating system paging files and other temporary files that serve no purpose if a system is restored, for example, need not be backed up.

The following are examples of some such files and folders that you can exclude from backups on a Windows 10 machine. If you're using backup software, the software likely comes with a built-in list of default exclusions that may resemble this list:

- **The Recycle Bin,** which effectively temporarily backs up deleted files in case a user changes his or her mind about deleting them
- **Browser caches,** which are temporary Internet files from web browsers, such as Microsoft Edge or Internet Explorer, Firefox, Chrome, Vivaldi, or Opera
- **Temporary folders,** which are often called Temp or temp and reside in c:\, in the user directory, or in the data directory of software
- **Temporary files,** which are usually named *.tmp or *.temp
- **Operating system swap files,** such as pagefile.sys

- **Operating system hibernation-mode system image information,** such as hyberfil.sys
- **Backups** (unless you want to back up your backups), such as Windows File History
- **Operating system files backed up during an operating system upgrade,** as usually found in C:\Windows.old on Windows computers that have had their operating systems upgraded
- **Microsoft Outlook cache files (*.ost),** but Outlook local data stores (*.pst) should be backed up (in fact, in many cases, they may be the most critical files in a backup)
- **Performance log files** in directories called PerfLogs
- **Junk files** that users create as personal temporary files to hold information, such as a text file in which the user types a phone number that someone dictated to him or her, but that the user has since entered into his or her smartphone directory

In-app backups

Some applications have built-in backup capabilities that protect you from losing your work if your computer crashes, power fails, or you don't have battery power left.

One such program is Microsoft Word, which offers users the ability to configure how often files should be saved for AutoRecover. For most people, this feature is quite valuable. The author of this book even benefited from this feature while writing this book!

While the mechanism of configuring AutoRecover varies between some versions of Word, in most modern versions, the process is the following or something similar: Choose File ⇒ Options ⇒ Save and configure the options according to your taste.

TIP In-app backups usually take just seconds to configure, normally run without your being actively involved, and can save you a lot of aggravation. In almost all cases, you should enable the feature if it exists.

Exploring Backup Tools

You can use multiple types of tools to create, manage, and restore from backups. Tools can automate various types of backups, for example, or can manage the process of a perpetual syncing backup. Backup tools come in wide variety of price ranges, depending on their robustness and scalability.

Backup software

Backup software is software designed specifically to run and manage backups and restorations from backups. You can find multiple vendors of such software, with exact features varying between products and between the platforms that they support (for example, features may vary between Windows and Mac versions of the same backup software package). Some offerings are intended for home users, some for large enterprises, and others for pretty much every level in between.

You can use backup software to manually or automatically backup — that is, you can configure it to backup specific systems, data, drives, or folders at specific times, using different backup models, such as full, incremental, and so on.

WARNING Backups can run only if a machine is on. So, be sure that your device to be backed up is on at those times! (Some backup software can be configured in cases of a missed backup to run the backup the next time that the device is booted or is idle.)

TIP Backup software can take some time to set up, but after you do so, it can often make the process of creating proper backups much easier than any other method of backing up.

Ideally, you should configure your systems to automatically back up at specific times to make sure that you actually back up and don't neglect doing so while you do any of the many things that come up in life.

WARNING Do not confuse these manual and automatic options with manual and automated task copying.

If you just worked on some important project or spent many hours creating some new work on your computer, however, you may want to kick off an extra manual backup to protect your work and the time that you invested in it.

TIP Beware of bogus backup software! Unscrupulous parties offer free backup software that contains malware of various severity, ranging from annoying adware to data-stealing infectors. Make sure that you obtain your backup software (as well as any other software that you use) from a reliable source.

Drive-specific backup software

Some external hard drives and solid state devices come with built-in backup software. Such software is often extremely intuitive and easy to use, and users may find it the most convenient way to set up their backup routines.

WARNING Three caveats, however:

- Remember not to leave the drive connected to the system holding the primary data store.
- If you use drive-specific versions of backup software, you may need to purchase all your backup drives from the same manufacturer in order not to complicate backup and restore procedures.
- Drive-specific software is less likely to support newer technologies as they emerge from other vendors than is general backup software.

Windows Backup

Windows comes equipped with basic backup software built in. The software sports several features, and, for many people, may be sufficient. Using Windows Backup is certainly better than not backing up at all.

You can configure Windows Backup in two places:

- In the Settings App, in the Update and Security Section.
- Via the traditional Control Panel, which can be run from the Start Menu. Backup and Restore is an item in the traditional All Items view or in the System and Security section of the modern view.

Additionally, a Windows File Backup utility automatically backs up files as you modify them. You can access its configuration options via the Control Panel File History option. If you have plenty of disk space and work efficiently, make sure that your files are backed up quite often.

For more on restoring files from Windows File History, see Chapter 15.

Smartphone/tablet backup

Many devices come equipped with the ability to automatically sync your data to the cloud — a process that allows you to restore the data to a new device if your device is lost or stolen. Even devices that do not have this feature built in almost always can run software that effectively delivers these features for a specific folder tree or drive.

Using the sync feature provides great protection, but it also means that your data is sitting *in the cloud* — which, simply means that it is on someone else's computer — and potentially accessible to both the cloud-

service provider (in the case of most smartphones, the provider would be Apple or Google), as well as to any government agencies that demand access to the relevant data while armed with a warrant, rogue insiders, or hackers who manage to somehow obtain access to it.

REMEMBER Even if you haven't committed any crimes, the government may still demand your data as part of data collection procedures related to crimes committed by other people. Even if you trust the government not to abuse your data, the government itself has had several breaches and data leaks, so you have good reason not to trust it to adequately protect your information from being stolen by other parties who may abuse it.

Before you decide whether or not to use the sync, think about the pros and cons.

Manual file or folder copying backups

Manual backups are exactly what they sound like: backups performed manually, often by people copying files, folders, or both from their primary hard drive (or solid-state drive) to a network folder or thumb drive.

WARNING Manual backups have their purpose, but using them on their own is not usually a good backup strategy. People inevitably do not perform such backups as frequently as they should, do not properly store such backups, and often do not back up all the items they should be storing copies of.

Automated task file or folder copying backups

Automated-task backups are essentially manual backups on steroids; they are manual backups that are run by a computer automatically instead of by people manually kicking them off. While automating the backup process reduces the risk of forgetting to back up or not backing

up due to someone being hurried, file and folder copying is still risky because if some sensitive information is, for some reason, not stored in the proper folder, it may not be backed up.

One possible exception is the case of virtual drives. If someone automates the process of copying of the file containing the entire drive on which he or she stores all of his or her data files, such backups may be sufficient. For most home users, however, setting up an automated copying routine is not a practical solution. Using backup software is a far simpler, and better, option.

Third-party backups of data hosted at third parties

If you store any data in the cloud or use a third-party service to host any of your systems or data, the party that owns the physical and/or virtual systems on which your data resides may or may not back it up — often without your knowledge or approval. If you store data on a Google Drive, for example, you have absolutely no control over how many copies Google makes of your data. Likewise, if you use a third-party service such as Facebook, any data that you upload to the social media giant's servers — regardless of the privacy settings that you set for the uploads (or possibly even if you deleted them) — may be backed up by Facebook to as many backups as the firm so desires, in as many different locations as the firm desires.

In some cases, third-party backups resemble drive backups. While the provider has your data backed up, only you — the party who "owns" the data — can actually read it in an unencrypted form from the backup. In other cases, however, the backed-up data is available to anyone who has access to the backup.

That said, most major third parties have robust redundant infrastructure and backup systems in place, meaning that the odds that data stored on their infrastructure will remain available to users is extremely high when compared with data in most people's homes.

Knowing Where to Back Up

For backups to have any value, they must be properly stored so they can be quickly and easily accessed when needed. Furthermore, improper storage of backups can severely undermine the security of information contained within the backups. You've probably heard stories of unencrypted backup tapes that contained sensitive information on them getting lost or stolen.

That said, there is not a one-size-fits-all approach to proper storage of backups. You can back up in different places, which results in different storage locations.

Local storage

Storing a *local copy* of your backup — meaning somewhere near a home computer or readily accessible to the owner of a smartphone, tablet, or laptop — is a good idea. If you accidentally delete a file, you can quickly restore it from the backup.

REMEMBER That said, you should never keep all your backups local. If you store your backups in your house, for example, and your house were to be severely damaged in a natural disaster, you could simultaneously lose your primary data store (for example, your home computer) and your backups.

Backups should always be stored in a secure location — not on a bookshelf. A fireproof and waterproof safe bolted down to the floor or fastened to the wall are two good options.

Also, keep in mind that hard drives and other magnetic media are less likely to survive certain disasters than solid-state drives, thumb drives, and other devices containing memory chips.

Offsite storage

Because one of the purposes of backing up is to have the ability to preserve data (and systems) even if your primary copy is destroyed, you want to have at least one backup *offsite* — meaning in a different location than your primary data store.

Opinions differ as to how far away from the primary store the backup should be kept. Essentially, the general rule is to keep the backups far away enough that a natural disaster that severely impacts the primary site would not impact the secondary.

TIP Some people store a backup copy of their data in a fireproof and waterproof bag inside a safe deposit box. Bank safes typically survive natural disasters, so even if the bank is relatively close to the primary site, the backup is likely to survive even if it cannot be retrieved for several days.

Cloud

Backing up the cloud offers the benefits of offsite storage. If you lose all your equipment and systems to a natural disaster, for example, a copy of your data will almost always still exist in the cloud. Also, from a practical standpoint, the odds are that the information-security team at any major provider of cloud storage has much greater knowledge of how to keep data secure than do most individuals and have at their disposal tools that the average person cannot afford to purchase or license.

At the same time, cloud-based backup has its drawbacks.

When using cloud-based backup, you are relying on a third-party to protect your data. While that party may have more knowledge and better tools at its disposal, its primary concern is not you. If a breach occurs, for example, and large customers are impacted, its priorities may lie in addressing their concerns before addressing yours. Also, major sites are often major targets for hackers because they know that such sites contain a treasure trove of data, far greater than what they may be able to lift from your home PC. Of course, if the government serves the cloud provider a warrant, law enforcement agents may obtain copies of your

backups — even, in some cases, if the warrant was served because it has demonstrated probable cause only that someone else (and not you) committed a crime.

That said, for most people, cloud-based backup makes sense, with the pros outweighing the cons, especially if you encrypt your backups, thereby making their contents inaccessible to the cloud provider.

REMEMBER When it comes to computers, *cloud* really means "someone else's computers." Anytime you store sensitive data, including sensitive data within in backups, in the cloud, you're really storing it on some physical computer belonging to someone else. The cloud provider may offer better security than you can offer yourself, but do not expect that your using the cloud will somehow magically eliminate cybersecurity risks.

Network storage

Backing up to a network drive offers a blend of features from several of the prior locations for storing backups.

Like a local backup, a network backup is normally readily available, but, perhaps, at a slightly lower speed.

Like an offsite backup, if the network server on which the backup is located is offsite, the backup is protected from site problems at the primary data's site. Unlike offsite backup, however, unless you know for sure that the files are offsite, they may be in the same facility as the primary data.

Like cloud backup, network based backup can be restored to other devices on your network. Unlike cloud backup, it may be accessible to only devices on the same private network (which, may be a problem, or, in some situations, a good thing from a security standpoint).

Also, network storage is often implemented with redundant disks and with automatic backups, offering better protection of your data that many other storage options.

TIP If you use network storage for backups, make sure that whatever mechanism you are using to run the backup (for example, backup software) has the proper network permissions to write to the storage. In many cases, you may need to configure a login and password.

Mixing locations

There is no reason to only back up to one location. From the perspective of restoring data quickly, the more places that you have your data securely backed up, the better. In fact, different locations provider different types of protection optimized for different situations.

Keeping one copy local so that you can quickly restore a file that you accidentally delete, as well as maintaining a backup in the cloud in case of natural disaster, for example, makes sense for many people.

Keep in mind, however, that if you do store backups in multiple locations you need to make sure all the locations are secure. If you can't be sure about the security of some form of backup, beware and do not back up there just because "the more backups, the better."

TIP As different backup locations provide different strengths and weaknesses, utilizing multiple backup locations can protect you better against more risks than using just one site.

Knowing Where Not to Store Backups

Never, ever, store backups attached to your computer or network, unless you have another backup that you are willing to recover in case of a

malware attack. Ransomware that infects your computer and renders the files on it inaccessible to you may do the same to your attached backup.

WARNING After backing up, never leave backup hard drives or solid-state drives connected to the systems or networks that they are backing up. Any malware that infects the primary system can spread to the backups as well. Removing your backup from being connected to the material that it is backing up can make all the difference between quickly recovering from a ransomware attack and having to pay an expensive ransom to a criminal.

If you back up to write-once, read-many-times type media, which is most commonly found today in the form of CD-Rs and DVD-Rs, it is safe to leave the backup in an attached drive after you have finalized the backup recording and set the disk to read-only.

Encrypting Backups

Backups can easily become a weak point in the data protection security chain. People who are diligent about protecting their personal information, and organizations that are careful to do the same with their confidential and proprietary information, often fail to afford the same level of protection to the exact same data when it resides in backups rather than in its primary location.

How often do we hear news stories, for example, of sensitive data put at risk because it was present in an unencrypted form on backups tapes that were lost or stolen?

TIP In general, if you’re not sure if you should encrypt your backup, you probably should.

Be sure to encrypt your backups if they contain any sensitive information, which, in most cases, they do. After all, if data is important enough to be backed up, the odds are pretty good that at least some of it is sensitive and should be encrypted.

Just be sure to properly protect the password needed to unlock the backups. Remember, it may be a while before you actually need to use the backups, so do not rely on your memory, unless you practice using that password on a regular basis to test the backups.

TIP From a practical standpoint, many professional system administrators who deal with multiple backups every day have never seen a backup that did not need to be encrypted.

Figuring Out How Often You Should Backup

No simple one-size-fits-all rule applies as to how often you should backup your system and data. In general, you want to ensure that you never lose enough work that it would cause you significant heartache.

Performing a full backup every day requires the most amount of storage space for backups and also takes the most time to run. However, doing so means that more total copies of data are available — so, if a backup were to go bad at the same time as the primary data store, less data is likely to be lost — and fewer backups are required to perform a system or data restoration.

Performing a full backup everyday may be feasible for many individuals, especially those who can run the backups after work hours or while they are asleep at night. Such a strategy offers the best protection. With storage prices plummeting in recent years, the cost of doing so, which was once prohibitive for most individuals, is now affordable to most folks.

Some people and organizations choose to perform a weekly full backup and couple that backup with daily incremental or differential backups. The former strategy provides the fastest backup routine; the latter offers the faster recovery routine and reduces the number of backups needed in order to perform a restore to a maximum of two instead of seven.

TIP Additionally, consider using manual backups or an automated in-app backup scheme if you are working on important materials during the day. Using the in-app automated backups in Word, for example, can protect you from losing hours of work if your computer crashes. Likewise, copying documents to a second location can prevent losing significant work if your hard drive or SSD fails.

For apps that do not have in-app-auto-backup capabilities, some folks have suggested periodically using the Windows or Mac Send menu option to send to themselves via email copies of files that they are working on. While doing so is clearly not a formal backup strategy, it does provide a way of backing up work during the day between regular backups and often does so offsite, ensuring that if one's computer were to die suddenly, an entire day's worth of work would not be lost.

TIP In general, if you are not sure if you are backing up often enough, you probably aren't.

Disposing of Backups

People and organizations often store backups for long periods of time — sometimes preserving materials for so long that the encryption used to protect the sensitive data on backup media is no longer sufficient to adequately protect the information from prying eyes.

As such, it is imperative that, from time to time, you either destroy your backups or re-create them.

REMEMBER Both hardware and software formats change over time. If you backed up to tapes in the 1980s, to Bernoulli Boxes in the early 1990s, or to Zip drives in the late 1990s, you may have difficulty restoring from the backups today because you may have problems obtaining the necessary hardware, compatible drivers, and other software needed to read the backups on a modern computer.

Likewise, if you backed up data along with various DOS programs or early Windows 16-bit executables needed to process the contents of those backups, you may be unable to restore from the backups to many modern machines that may be unable to run the executables. Obviously, if you did a full system image of a machine 20 years ago, you are going to have difficulty restoring from the image today (you may be able to do so using virtual machines — something well beyond the technical skill level of most users).

Even some older versions of data files may not work easily. Word documents from the mid-1990s, for example, which can be infected with various forms of malware, do not open in modern versions of Word unless a user enables such access, which may be difficult or impossible to do in certain corporate environments. Files formats utilized specifically by software that has long since disappeared entirely from the market may be even harder to open.

As such, old backups may not have much value to you anyway. So, once a backup is no longer valuable or once its data protection may be at risk of compromise, get rid of it.

How should you dispose of the backup tapes, disks, and so on? Can you just throw them in the trash?

No. Do not. Doing so can totally undermine the security of the data in the backups.

Instead, utilize one of the following methods:

- **Overwriting:** Various software programs will write over every sector of the storage media several times (the actual number of times depends on the security level that the user specifies), making subsequent recovery of data from the decommissioned media difficult, if not impossible.
- **Degaussing:** Various devices containing strong magnets can be used to physically render data on magnetic media (such as hard drives and floppy disks) inaccessible by exposing the media to a strong magnetic field.
- **Incineration:** Burning storage media in a high-temperature fire is often enough to destroy it. Do not attempt this on your own. If you want to pursue such a method, find a professional with experience. The incineration process varies based on the type of media involved.
- **Shredding:** Cutting the media into tiny pieces. Ideally, such media should be totally pulverized into dust. In any case, shredding using an old-fashioned shredder that cuts media into strips is generally not considered secure disposal of media that has not been previously overwritten or degaussed.

TIP I can’t overstate the importance of properly storing and disposing of backups. Serious data leaks have resulted from backup media that was lost after being stored for quite some time.

Testing Backups

Many folks have thought that they had proper backups only to discover at the time that they needed to restore that the backups were corrupted. Hence, testing backups is critical.

While, theoretically, you should test every backup that you make and test that every single item within the backup can be restored, such a

scheme is impractical for most people. Do, however, test the first backup that you make with any software, check the auto-recover files the first time that you use Word, and so on.

Some backup software comes with the capability to *verify* backups — that is, after making a backup, it checks that the original data and data in the backups match. Running such verification after making a backup adds significant time to the backup process, but is well worth running if you can do so because it helps ensure that nothing was improperly recorded or otherwise became corrupted during the backup process.

Conducting Cryptocurrency Backups

Because cryptocurrency (see Chapter 1) is tracked on a ledger and not stored in a bank, backing up cryptocurrency involves backing up the private keys used to control the addresses in the ledger at which one has cryptocurrency, not backing up the cryptocurrency itself. Often, keys are not maintained electronically. They're printed on paper and stored in a bank vault or fireproof safe.

For those who use hardware wallets to store the keys to their cryptocurrency, the backup for the wallet device is often a *recovery seed*, which is a list of words that allows the device to re-create the keys needed for the relevant addresses. It is generally accepted that the list of words should be written down on paper and stored in a bank vault and/or safe — not stored electronically.

Backing Up Passwords

TIP Anytime that you back up lists of passwords, make sure to do so in a secure manner. For important passwords that do not change often and are not likely to be needed on an urgent basis, consider making no digital records of them at all. Instead, write them down on a piece of paper and put that paper in a bank safe deposit box.

Creating a Boot Disk

If you ever need to re-create your system, you will need the ability to boot the computer, so as part of the backup process, you should create a boot table disk. For most smartphones and tablets, creating a boot disk is not an issue because resetting the device to factory settings will make it bootable.

Such simplicity is not, however, always the case with computers, so when you perform your first backup you should ideally make a bootable disk that you know is safe to boot from (in other words, no malware and so on). Most backup software packages will walk you through this process, and some computer manufacturers will do the same on your initial startup of the system. Various security software packages are distributed on bootable CDs or DVDs as well.

Chapter 14

Resetting Your Device

IN THIS CHAPTER

- **Discovering two major types of device resets**
- **Figuring out when you should use each type to reset your device**
- **Resetting your device accordingly**

Chapter 13 talks about backing up and why it is a critical component of any and every cybersecurity plan. The odds are close to 100 percent that, at some point, you will lose access to some file to which you still need access, and restoring from a backup will be a "lifesaver."

In this chapter, I discuss resetting your computer and tell you what you need to know to successfully reset your device so that it's (almost) as good as new.

Exploring Two Types of Resets

Sometimes, the easiest way to restore — and to help ensure that none of the problems that forced you to restore in the first place remain — is to start over by resetting your device to factory settings and reinstalling your apps and copying your data files from a backup.

TIP Some forms of malware can survive a factory reset. So, if your device was infected with malware, be sure to address that problem even if you plan to reset your device. Or consult with an expert.

Additionally, there will likely be times when your device crashes — that is, it becomes unresponsive and stops functioning normally. Such occasions can be scary for many nontechnical users, who assume that

they may lose their data. Performing the proper type of reset in such occasions, however, is quite simple and will almost always preserve the user's files (although files currently being worked on may be preserved as they were last saved).

Resets come in two major flavors— soft and hard. It is critical to know the difference between them before you use either type.

Soft resets

A *soft reset* is the equivalent of physically turning a device off and then turning it back on. It does not wipe programs, data, or malware.

TIP One common use of soft resets is to restart a device if it crashes and becomes unresponsive. It can also be useful after a Blue Screen of Death-type of crash (see Figure 14-1).

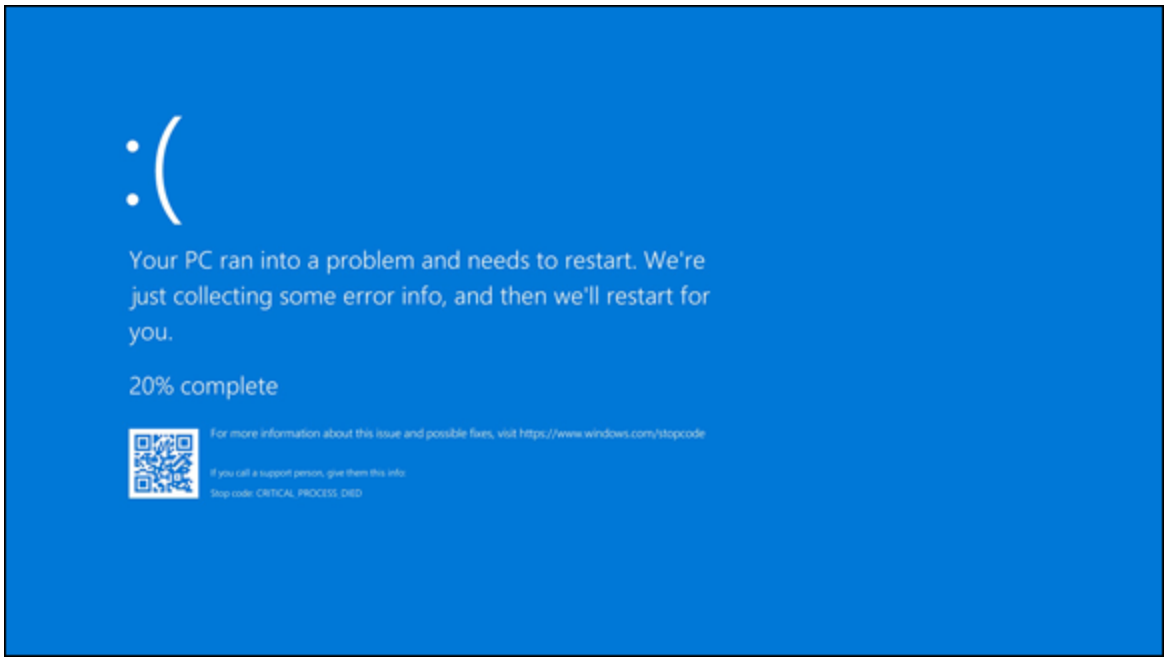

FIGURE 14-1: One variant of the infamous Windows Blue Screen of Death. If you see this screen, you need to soft reset your computer.

Older devices

Most modern computing devices have a soft reset capability, but some older devices do not. In such devices, however, the battery is often removable, so removing the battery and cutting off all power to the device achieves the same desired effect.

Windows computers

Most Windows computers can be soft reset by holding down the Power button for ten seconds to do a shutdown. Holding down the button cuts off power to the computer from both the battery and any connected AC adapters/mains (even if the battery is connected and fully charged) and shuts it down.

After the device shuts down, wait ten seconds and press the Power button once to restart the computer.

Mac computers

Various models of Mac computers can be soft reset through different means:

- Hold down the Power button for about five seconds, and the Mac should shut down completely. Let go of the Power button, wait a few seconds, and press it once again, and the Mac should reboot. On some Macs pressing and holding the Power button may display a menu, in which case you should press R for Reboot and reboot directly, rather than shutting down and restarting the device.
- Press and hold the Control + ⌘ key together with the Power button.
- Press and hold the TouchID button until the Mac reboots.

Android devices

The way to soft reset an Android device varies between manufacturers. One of the following methods is likely to work:

- Press and hold the Power button until you see a shutdown/restart menu and then press Restart. (Or press Power Off, wait a few seconds, and then press the Power button again to turn the phone back on.)

- Press and hold the Power button. If no menu appears, keep holding the Power button for 2 minutes. At some point the phone should turn off — when it does, wait 10 seconds and turn it back on.
- If you have a removable battery, remove it, wait ten seconds, put it back in, and turn on the phone.

iPhones

The way to soft reset an iPhone varies based on the model. In general, one of the following methods will work:

- Press and release the Volume Up button, then press and release the Volume Down button, and then press and hold the Side button (the Power button) until the Apple logo appears on the screen. Wait for the device to reboot.
- Press and hold the Power button. While still holding it, press and hold the Volume Down button. When a Slide To Power Off prompt and slider appears on the screen, slide the slider to the right and turn the device off. Wait ten seconds and press the Power button to turn it back on.
- Press and hold the Power button, and, while still doing so, press and hold the Volume Down button. Continue to hold both buttons as the iPhone powers off and back on. Release both buttons when the Apple logo appears on the screen and wait for the device to reboot.

  

  WARNING If you are using some versions of the iPhone X, following this option for performing a soft reset could end up calling emergency services (911 in the United States) because holding these particular buttons for longer than five seconds may be preprogrammed to issue an SOS signal from the device.

Hard resets

Hard resets reset a device to its factory image or to something similar. (For more on factory image, see Chapter 13.)

If you want to recover to the original factory image — to effectively reset your device to the way it was when it was new — you need to follow the instructions for your particular device.

WARNING Hard resets are almost always irreversible. Once you run a hard reset and a device is set back to its factory settings, you typically cannot undo the reset. Anything that you previously installed on the device and any data that you stored on it is likely gone forever. (Advanced tools may, in some cases, be able to recover some of the material, but such recoveries are often incomplete, and, in many cases, impossible altogether.) As such, do not run a hard reset until you are sure that you have backups of all the material that you need on the device that you are hard resetting.

Also keep in mind the following:

- In some cases, a factory reset will not reset your device to the way it was when it was new because during operating system updates, the recovery image was updated as well. Factory resetting such a device will set the device to the way the device would have looked (or quite similar to the way it would have looked) when it was new had you purchased it with the new operating system.
- After performing a factory reset, one or more (or possibly all) patches and other security updates that you have installed on the device may be gone — meaning that your device is more likely than not vulnerable to various compromises. So, immediately after restoring you should run the operating system update process (repetitively — until it finds no needed updates) as well as the update process for any security software (also repetitively until it finds no needed updates). Only after those steps have been completed should you begin to install other software or perform any other online activities.

Resetting a modern Windows device

Your modern Windows device likely offers one or more ways to reset it. The following sections describe three major ways.

METHOD 1

1. **In the Start menu, click on Settings or PC Settings, depending on your operating system version.**
2. **In Windows Settings, click on Update and Security.**

   The Windows Update screen appears.
3. **Click on Recovery in the menu on the left side of the Window.**
4. **Click on the Get Started button in the Reset this PC section at the top of the window.**

   At this point, you may be prompted to install the original installation CD on which you received Windows 10. If you receive that message, do so. If you do not receive it — and most users don't — just continue.

   Windows then offers you two choices. Both remove programs and apps and reset settings to their defaults:

   - **Keep my files:** Selecting this option leaves your data files intact (as long as they are stored in data folders).
   - **Remove everything:** Selecting this option removes all your data files along with the apps and programs (this is the factory reset option).
5. **Select either reset option.**

If you're performing a full reset because your system was infected by malware or your data files may otherwise have been corrupted, ideally select Remove everything and restore your data files from a clean backup.

If you select to remove your files along with everything else, Windows presents you with two choices:

- **Just remove my files:** Selecting this option erases your files, but does not perform any drive cleaning. This means that someone who gains access to the drive may be able to recover the data that was in the files — in full or in part — even after the files are deleted by the rest. This option runs relatively quickly.
- **Remove files and clean the drive:** Selecting this option not only removes all your data files, it wipes the drive — that is, writes over every 1 or 0 in your file — to dramatically reduce the likelihood that anyone in the future could recover any data from the deleted files. Cleaning a drive is time-consuming; if you select this option the restore can take much longer than if you select the first option.

TIP If you are resetting the system so that you can use a clean system after recovering from a malware infection, there is no reason to clean the drive. If you are wiping it before giving it to someone else, fully cleaning the drive is a good idea. (In fact, some would argue that you should wipe the entire drive with even better wiping technology than is provided through the reset option discussed in this chapter.)

At this point, you may receive a warning message. If your computer originally had a different operating system and was upgraded to Window 10, resetting the system will remove the recovery files created during the upgrade that allow you to downgrade back to the previously running operating system — meaning that if you reset the system you will have a Windows 10 computer that cannot be easily downgraded to another operating system. In most cases, this warning is not a significant issue — Windows 10 is relatively mature, and few people who upgrade to Windows 10 as of the data of this book's publishing choose to downgrade.

Of course, if you are resetting the system because it is not working properly after you performed an upgrade to Windows 10, do not

proceed with the reset. Downgrade it to the older version of Windows using the relevant tool.

You then will see a final warning message that tells you that the computer is ready to reset — and which communicates what that means. Read what it says. If you do not want any of the things that it says will happen to happen, do not proceed.

6. **When you are ready to proceed, click on the Reset button.**

   You can probably go out for coffee. A reset takes quite some time, especially if you chose to clean your drive.

7. **After a while, if you receive a prompt asking you whether you want to continue to Windows 10 or to perform troubleshooting, click on Continue.**

METHOD 2

If you're *locked out* of your computer, meaning that it boots to a login screen, but you cannot log in — for example, if a hacker changed your password — you can still factory reset the machine:

1. **Boot your PC.**
2. **When the login screen appears, click on the Power icon in the bottom right-hand corner.**

   You are prompted with several choices. Do not click on them yet.

3. **Without clicking any choices, first hold down the Shift key and then click on Restart.**

   A special menu appears.

4. **Click on Troubleshoot.**
5. **Select Reset This PC.**
6. **Select Remove Everything.**

WARNING Read the warnings, and understand what the consequences of running a hard reset are before you run it. This reset is likely irreversible.

METHOD 3

This method may vary a bit between various computer manufacturers.

To reset your device:

1. **Turn on your computer and boot into Windows 10.**

   If you have more than one operating system installed on your computer, select the Windows 10 installation that you want to reset. If all you have is one operating system — as is the case for most people — you won't have to select it because it will boot automatically.

2. **While the computer is booting, press and hold down the F8 key to enter the boot menu.**
3. **In the boot menu on the Advanced Boot Options screen that appears, click on Repair Your Computer and press Enter.**
4. **If you're prompted to choose a keyboard layout, do so and then click on Next.**
5. **Select your username, type your password, and click on OK.**
6. **From the System Recovery Options menu that appears, click on the System Image Recovery link and follow the onscreen prompts to do a factory reset.**

TIP If your menus appear differently after pressing F8 in the last step, look through them for a Factory Reset option.

Resetting a modern Android device

Modern Android devices come equipped with a Factory Reset feature, although the exact location of the activation option for it varies based on the device's manufacturer and operating system version.

I show you several examples of how to activate a hard reset on several popular devices. Other devices are likely to have similar options.

SAMSUNG GALAXY SERIES RUNNING ANDROID 9

On popular Samsung Galaxy phones running Android version 9 (or Android Pie, the latest version of Android as of early 2019), you can access the factory reset option by following these instructions:

1. **Run the Settings app.**
2. **From the main Settings menu, click on General Management.**
3. **Click on Reset.**
4. **Click on Factory Data Reset.**
5. **Follow the instructions presented with the relevant warning.**

SAMSUNG TABLETS RUNNING ANDROID 9

The popular Samsung series of tablets have menu structures for hard-resetting that are similar to those used for the Galaxy series, although with a different look and feel.

1. **Run the Settings app.**
2. **From the main Settings menu, click on General Management.**
3. **In the General Management menu, click on Reset.**
4. **Click on Factory Data Reset.**
5. **Follow the instructions at the warning to continue.**

HUAWEI DEVICES RUNNING ANDROID 8

Huawei phones, which are popular throughout Asia, can be reset using the following steps (or similar steps, in case of operating system version differences):

1. **Run the Settings app.**

2. **From the main settings menu, click on System.**
3. **In the System menu, click on Reset.**
4. **In the Reset menu, click on Factory Data Reset.**
5. **Follow the instructions at the warning to continue.**

Resetting a Mac

Before you hard reset a Mac, you should perform the following steps:

1. **Sign out of iTunes.**
2. **De-authorize any apps that are locked to your Mac.**

   Sign out of them so that you can relog-in from the newly restored device, which those systems may see as if it were a different device.
3. **Sign out of Messages.**
4. **Sign out of iCloud.**

   You can do this in the System Preferences app. You will need to put in your password.

While a hard reset will work without the preceding three steps, performing the steps can prevent various problems when you restore.

After you're signed out of iTunes, Messages, and iCloud:

1. **Restart your Mac in Recovery Mode by restarting your Mac and holding down the Command and R keys while it reboots.**

   You may be presented with a screen asking you in what language you want to continue. If you are, select your preferred language — for the sake of this book, I assume that you have selected English.
2. **Run the Disk Utility.**
3. **In the Disk Utility screen, select your device's main volume and click on Unmount then Erase.**
4. **Erase any other disks in the device.**
5. **Exit the Disk Utility by clicking Quit Disk Utility in the Disk Utility menu.**

6. **Click on Reinstall macOS and follow the steps to reinstall the operating system onto the primary disk within your Mac (see Figure 14-2).**

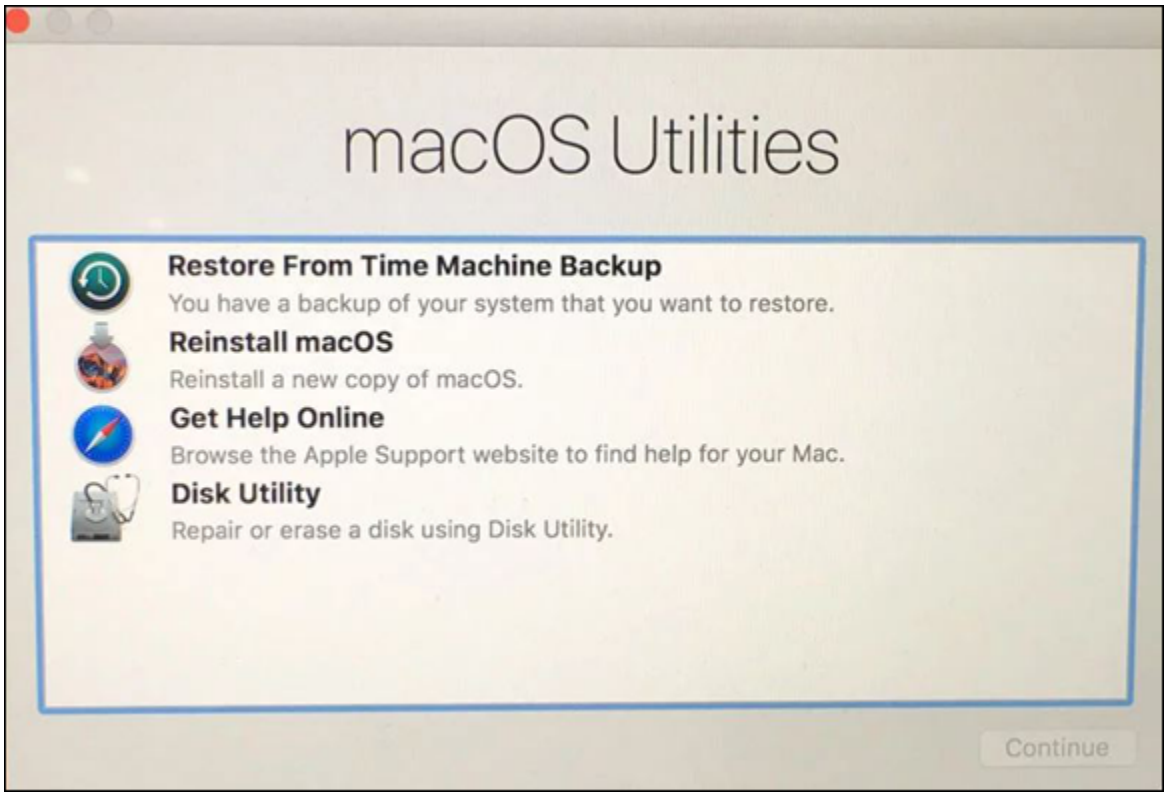

FIGURE 14-2: The Mac Recovery Mode menu.

Resetting an iPhone

To hard reset a modern iPhone:

1. **Run the Settings app and choose General ⇒ Reset ⇒ Erase All Content and Settings.**
2. **If you're asked for your Apple ID and Password to confirm the erasure, enter them.**
3. **When you see a warning and a red Erase iPhone (or iPad) button, click on it.**

Rebuild Your Device after a Hard Reset

After you hard reset a device, you should

- Install all security updates
- Install all the programs and apps that you use on the device — and any relevant updates
- Restore your data from a backup

See Chapter 15 for more detail on these topics.

Chapter 15

Restoring from Backups

IN THIS CHAPTER

- **Restoring from different types of backups**
- **Figuring out archives**
- **Recovering cryptocurrency**

Backing up is a critical component of any and every cybersecurity plan. After you reset a device to its factory settings as part of the recovery process (see Chapter 14), you can restore your data and programs so that your device will function as normal.

Because most people do not have to restore from backups regularly and because restoration is typically done after something "bad" happened that forced the restoration to be necessary, many folks first experience the process of restoring from backups when they are quite stressed. As such, people are prone to making mistakes during restoration, which can lead to data being lost forever. Fortunately, this chapter shows you how to restore.

You Will Need to Restore

The odds are close to 100 percent that, at some point, you will lose access to some file to which you still need access, and restoring from a backup will be a lifesaver. But restoring is not necessarily simple. You need to contemplate various factors before performing a restoration. Proper planning and execution can make the difference between recovering from lost data and losing even more data.

TIP Restoring from backups is not as simple as many people think. Take the time to read this chapter before you perform a restore.

Wait! Do Not Restore Yet!

You noticed that some data that you want to access is missing. You noticed that a file is corrupted. You noticed that some program is not running properly. So, you should restore from a backup, right? Wait!

WARNING Restoring without knowing why the problem occurred in the first place may be dangerous. For example, if you have a malware infection on your computer, restoring while the malware is still present won't remove the threat, and, depending on the type of malware and backup, may lead to the files in your backup becoming corrupted as well. If the malware corrupts the primary data store, you may lose your data and have nowhere from which to restore it!

For example, people who tried to restore data from backups on external hard drives have lost data to ransomware. The moment the external drive was connected to the infected computer, the ransomware spread to the backup and encrypted it as well!

WARNING Malware can spread to cloud-based storage as well. Merely having the backup in the cloud is not a reason to restore before knowing what happened.

Even in the case of backups that are on read-only media, which malware cannot infect, attempting to restore before neutralizing the threat posed

by the infection can waste time and potentially give the malware access to more data to steal.

Before you restore from any backups, make sure to diagnose the source of the problem that is causing you the need to restore. If you accidentally deleted a file, for example, and know that the problem occurred due to your own human error, by all means go ahead and restore. But if you're unsure what happened, apply the techniques described in Chapters 11 and 12 to figure out what you need to do to make your computer safe and secure prior to restoring from the backup.

Restoring from Full Backups of Systems

A *full system backup* is a backup of an entire system, including the operating system, programs/apps, settings, and data. The term applies whether the device being backed up is a smartphone or a massive server in a data center.

As such, the restoration process recreates a system that is effectively identical to the one that was backed up at the time that it was backed up. (This is not totally true in the absolute sense — the system clock will show a different time than the original system, for example — but it is true for the purposes of learning about system restoration.)

Restoring to the computing device that was originally backed up

System restoration from a system image works best when systems are restored to the same computing device from which the original backup was made. If your system was infected with malware, for example, and you restore to the same device from an image created before the malware infection took place, the system should work well. (Of course, you would lose any work and other updates done since that time, so hopefully you backed them up using one of the methods in Chapter 13.)

WARNING Full system restores are often irreversible. Be absolutely sure that you want to run one before you do.

Restoring from a full system backup is likely the fastest way to restore an entire system, but the process can take dramatically longer than restoring just a few files that were corrupted. It is also far more likely to lead to accidentally erasing settings or data created since the last backup. As such, use a full system restore only when one is truly needed.

TIP If you accidentally delete a bunch of files or even folders, do not perform a full system restore. Just restore those files from a backup using one of the techniques described later in this chapter.

Restoring to a different device than the one that was originally backed up

REMEMBER System restoration from an image often won't work on a system with totally different hardware components than the system that was originally imaged. In general, the more different a system is from the system that was imaged, the more problems that you may encounter.

Some of those problems may autocorrect. If you restore a system with drivers for one video card to a system with another video card, for example, the restored system should realize that the wrong drivers are installed and simply not use them. Instead, it defaults to the operating system's built-in drivers and allows you to install the drivers for the correct card (or, in some cases, automatically download them or prompt you to do so).

Some problems may not autocorrect. For example, if the computer that was backed up used a standard USB-connected keyboard and mouse and the device to which you are restoring uses some proprietary keyboard that connects differently, it may not work at all after the restore; you may need to attach a USB keyboard to the system to download and install the drivers for your proprietary keyboard. Such situations are becoming increasingly rare due to both standardization and improvements in modern operating systems, but they do exist.

Some problems may not be correctable. If you try to restore the system image of a Mac to a computer designed to run Windows, for example, it won't work.

TIP Some backup software packages allow you to configure a restore to either install separate drivers or search for drivers that match the hardware to which the restoration is being done to replace those found in the backup that are unsuitable. If you have such a feature and have difficulty restoring without it, you may want to try it.

A full system backup may or may not include a backup of all content on all drives attached to a system, not just those mounted inside of it. (Theoretically, all such drives should be included in a system image, but the term *system image* is often used to mean an image of the internal hard drives and SSDs.)

TIP If a device for which you have an image fails, you should be able to use the system image to re-create the entire system as it was at the time that the backup was made. When you use the rebuilt system, it should function exactly as the previous system did at the time of the backup.

Original system images

If you want to recover to the original factory image of a system prior to restoring your data and programs, see Chapter 14, which is dedicated to performing such restorations.

After performing such a factory reset, one or more (or possibly all) patches and other security updates that you have installed on the device may be gone. Your device is likely vulnerable to various compromises. Immediately after restoring, you should, therefore, run the operating system update process (repetitively until it finds no needed updates) as well as the update process for any security software (also repetitively until it finds no needed updates).

Only after those steps are completed should you install other software, restore your data, or perform any other online activities.

Later system images

Before you restore from any system image, you must ascertain that whatever problem occurred that necessitated the restoration will not remain, or be restored, during the restoration. If your computer was infected with ransomware, for example, and you remove the malware with security software, but need to restore the criminally encrypted files from a backup, you do not want to end up restoring the ransomware along with the data.

If you know for certain that an image was made prior to the arrival of the problem, go ahead and use it. If in doubt, if possible, restore to an extra device and scan it with security software prior to performing the actual restoration. If you do not have an extra device to which you can restore and are unsure as to whether the backup is infected, you may want to hire a professional to take a look.

Installing security software

After you restore from a system image (whether factory settings or a later image), the first thing that you should do is check whether security software is installed. If it is not, install it. Either way, make sure to run the auto-updates until the software no longer needs updates.

TIP Install security software before attempting to do anything online or read email. If you do not have security software in place before you perform such tasks, performing them could lead to a security breach of your device.

If you have the security software on CD or DVD, install it from there. If you created a USB drive or other disk with the security software on it, you can install it from there. If not, copy the security software to the hard drive from wherever you have it and run it.

Original installation media

For programs that you acquire and install after you purchased your device, you can reinstall them after you restore the original system image or even a later image that was created before the software was installed.

TIP If you reinstall software from a CD or DVD, any updates to the software that were released after the CD or DVD was created will not be installed. Be sure to either configure your program to auto-update or manually download and install such updates. In some cases, software installation routines may also ask you whether you want them to automatically perform a check for updates immediately upon the completion of the installation. In general, answering affirmatively is a wise idea.

Downloaded software

The way that you reinstall programs that you previously purchased and installed at some point after you purchased your device depends on where the software is located:

- **If you have a copy of the software on a thumb drive,** you can reinstall from the drive by connecting it into your device, copying

the files to your hard drive, and running the install.

TIP If there is any possibility that the thumb drive is infected with malware — for example, you're restoring due to a malware infection and may have inserted the thumb drive into your infected computer at some point in the past — make sure to scan it with security software before you run or copy anything from it. Do so from a device with security software running that will prevent infections from spreading upon connection from the drive to the machine being used for scanning.

- **If you copied the software to a DVD or CD,** you can install from that disc. Make sure to install all necessary updates.
- **If the purchased software can be redownloaded from a virtual locker,** do so. In some cases, software that is redownloaded will have been automatically upgraded to the latest release. In other cases, it will be the same version as you originally purchased, so make sure to install updates.
- **If the software is downloadable from its original source** (public domain software, trialware that you activate with a code, and so on), feel free to redownload it. In some cases — for example, if newer versions require paying an upgrade fee —you may need to download the version that you had previously. In any case, make sure to install all updates for the version that you do install.

Restoring from full backups of data

In many cases, it makes sense to restore all the data on a device:

- **After a restore from a factory image:** After restoring from a factory image and reinstalling all necessary software, your device will still have none (or almost none) of your data on it, so you need to restore all your data.

- **After certain malware attacks:** Some malware modifies and/or corrupts files. To ensure that all your files are as they should be, after an infection, restore all your data from a backup. Of course, this assumes that you have a recent enough backup from which to do so without losing any work.
- **After a hard drive failure:** If a hard drive fails, in full or in part, you will want to move your files to another drive. If you have a separate drive for data than for the operating system and programs — as many people do — performing a full restore of data is the easiest way to restore.
- **When transitioning to a new, similar device:** Restoring from a backup is an easy way to ensure that you put all your data files onto the new device. Because some programs store settings in user data folders, copying the files directly or performing a selective restoration from a backup is usually a better way to go. But as people sometimes inadvertently leave out files when using such a technique, full restorations are sometimes used.
- **After accidental deletions:** People occasionally accidentally delete large portions of their data files. One easy way to restore everything and not worry about whether everything is "back to the way that it should be" is to do a full restore of all data.

Unlike restoring from a full system backup, restoring from a full data backup won't restore applications. If a system has to be rebuilt entirely, recovering from full backups of data likely requires prior restorations to factory settings (or a later image of the computer) and reinstallation of all software.

TIP The multi-step process of restoring from a factory image and then reinstalling applications and restoring data may seem more tedious than simply restoring from a more recent system image, but it also usually proves to be far more portable. Recovery can usually be done on devices that vary quite a bit from the original device, using images of those devices (or onto a new device), followed by the reinstallation of programs and the restoration of data.

Restoring from Incremental Backups

Incremental backups are backups made after a full backup and contain copies of only the portion of the contents being backed up that have changed since the preceding backup (full or incremental) was run.

TIP Some simplistic backup software products use incremental and differential backups internally, but hide the internal workings from users. All users do is select which files or file types to restore and, if appropriate, which versions of those files, and the system works like magic hiding the merging of data from multiple backups into the resulting restoration.

Incremental backups of data

In many cases of home users, *incremental backup* refers to incremental backups of data. To recover data that was backed up using an incremental backup scheme requires multiple steps:

1. **A restoration must be done from the last full data backup.**
2. **After that restoration is complete, restoration must be performed from each incremental backup performed since that**

last full backup.

Failing to include any of the incremental backups necessary in Step 2 may lead to corrupt data, missing data, data being present that should not be, or inconsistent data.

WARNING Most modern backup software will warn (or prevent) you if you try to skip any incremental backups during an incremental restoration. Such software, however, sometimes does not, however, tell you if you're missing the final backup or backups in a series.

Incremental backups of systems

Incremental system backups are essentially updates to system images (or partial system images in the case of partial backups) that bring the image up to date as of the data that the backup was made. The incremental system backup contains copies of only the portion of the system that changed since the preceding backup (full or incremental) was run.

To restore from an incremental backup of a system:

1. **A restoration must be done from the last full system backup.**
2. **After that restoration is complete, restoration must be performed from each incremental backup performed since that system image was created.**

Failing to include any of the incremental backups necessary in Step 2 may lead to corrupt of missing programs, data, operating system components, and incompatibility issues between software. Most modern backup software will warn (or prevent) you if you try to skip various incrementals during a restore from an incremental backup. They often do not, however, tell you if you're missing the final backup or backups in a series.

Differential backups

Differential backups contain all the files that changed since the last full backup. (They are similar to the first in a series incremental backups run after a full backup.)

TIP While creating a series of differential backups usually takes more time than creating a series of incremental backups, restoring from differential backups is usually much simpler and faster.

To recover from a differential backup:

1. **Perform a restoration from the last full system backup.**
2. **After that restoration is complete, perform a restoration from the most recent differential backup.**

Be sure to restore from the last differential backup and not from any other differential backup.

TIP Many backup systems won't warn you if you attempt to restore from a differential backup other than the latest one. Be sure to double-check before restoring that you're using the latest one!

Table 15-1 shows the comparative restoration processes from full, incremental, and differential backups.

TABLE 15-1 Restoration Processes

	Full Backup	*Incremental Backup*	*Differential Backup*
After Backup #1	Restore from Backup #1	Restore from Backup #1 (Full)	Restore from Backup #1 (Full)
After Backup #2	Restore from Backup #2	Restore from Backups #1 and #2	Restore from Backups #1 and #2

	Full Backup	*Incremental Backup*	*Differential Backup*
After Backup #3	Restore from Backup #3	Restore from Backups #1, #2, and #3	Restore from Backups #1 and #3
After Backup #4	Restore from Backup #4	Restore from Backups #1, #2, #3, and #4	Restore from Backups #1 and #4

Continuous backups

Some continuous backups are ideal for performing system restore. Similar to a system image, they allow you to restore a system to the way that it looked at a certain point in time. Others are terrible for performing restores because they allow restoration to only the most recent version of the system, which often suffers from the need to be rebuilt in the first place.

In fact, the normal use of continuous backups is to address equipment failures, such as a hard drive suddenly going caput — not the rebuilding of systems after a security incident.

Furthermore, because continuous backups constantly propagate material from the device being backed up to the backup, any malware that was present on the primary system may be present on the backup.

Partial backups

Partial backups are backups of a portion of data. Likewise, partial backups are not intended to be full backups in case of a malware attack or the like. They are useful, however, in other situations, and you should be aware of how to restore from them.

If you have a particular set of files that are extremely sensitive and need to be backed up and stored separately from the rest of your system, you may use a partial backup for that data. If something happens and you need to rebuild a system or restore the sensitive data, you will need that separate partial backup from which to do the restore.

Digital private keys that provide access to cryptocurrency, email encryption/decryption capabilities, and so on, for example, are often

stored on such backups along with images of extremely sensitive documents.

Often, partial backups of sensitive data are performed to USB drives that are then locked in safes or safe deposit boxes. Restoring from the backup would, in such cases, demand that the restorer obtain the physical USB drive, which could mean a delay in restoration. If the need to restore arises at 6 p.m. Friday, for example, and the drive is in a safe deposit box that is not available until 9 a.m. Monday, the desired material may remain inaccessible to the user for almost three days.

REMEMBER Make sure that you store your partial backups in a manner that will allow you to access the backed-up data when you need it.

Another common scenario for specialized partial backups is when a network-based backup is used — especially within a small business — and a user needs to ensure that he or she has a backup of certain material in case of technical problems while traveling. Such backups should never be made without proper authorization. If permission has been obtained and a backup has been created, a user on the road who suffers a technical problem that requires restoration of data can do the restore by copying the files from the USB drive (after, presumably, decrypting the files using a strong password or some form of multifactor authentication).

Folder backups

Folder backups are similar to partial backups because the set of items being backed up is a particular folder. If you performed a folder backup using a backup tool, you can restore it using the techniques described in the preceding section.

The restore process is different if, however, you created the relevant backup by simply copying a folder or set of folders to an external drive (hard drive, SSDs, USB drive, or network drive).

Theoretically, you simply copy the backup copy of the folder or folders to the location of the original folder. However, doing so will potentially overwrite the contents of the primary folder, so any changes made since the backup will be lost.

Drive backups

A *drive backup* is similar to a folder backup, but an entire drive is backed up instead of a folder.

If you backed up a drive with backup software, you can restore it via that software.

If you backed up a drive by copying the contents of the drive somewhere else, you will need to manually copy them back. Such a restore may not work perfectly, however. Hidden and system files may not be restored, so a bootable drive backed up and restored in such a fashion may not remain bootable.

Virtual-drive backups

If you backed up an encrypted virtual drive, such as a BitLocker drive that you mount on your computer, you can restore the entire drive in one shot or restore individual files and folders from the drive.

Restoring the entire virtual drive

To restore the entire virtual drive in one shot, make sure the existing copy of the drive is not mounted. The easiest way to do so is to boot your computer and not mount any Bitlocker drives.

If your computer is booted already and the drive is mounted, simply dismount it:

1. **Choose Startup ⇒ This PC.**
2. **Locate the mounted Bitlocker drive.**

   The drive appears with an icon of a lock indicating that it is encrypted.
3. **Right-click on the drive and select Eject.** Once the drive is dismounted, it disappears from the This PC list of drives.

After the drive is unmounted, copy the backup copy of the drive to the primary drive location and replace the file containing the drive.

You can then unlock and mount the drive.

Restoring files and/or folders from the virtual drive

To restore individual files or folders from the virtual drive, mount the backup as a separate virtual drive and copy the files and folders from the backup to the primary as if you were copying files between any two drives.

TIP Ideally, you should back up the backup of the virtual drive before mounting it and copying files and/or folders from it and mount it read-only when you mount it.

TIP Always unmount the backup drive after copying files to the primary. Leaving it mounted — which inherently means that two copies of a large portion of your file system are in use at the same time — can lead to human mistakes.

Dealing with Deletions

One of the problems of restoring from any restore that does not entirely overwrite your data with a new copy is that the restore may not restore deletions.

For example, if after making a full backup, you delete a file, create ten new files, modify two data files, and then perform an incremental backup, the incremental backup may or may not record the deletion. If you restore from the full backup and then restore from the incremental, the restore from the incremental should delete the file, add the ten new files, and modify the two files to the newer version. In some cases,

however, the file that you previously deleted may remain because some backup tools do not properly account for deletions.

Even when this problem happens, it is not usually critical. You just want to be aware of it. Of course, if you've deleted sensitive files in the past, you should check whether a restoration restored them to your computer. (If you intend to permanently and totally destroy a file or set of files, you should also remove it/them from your backups.)

Excluding Files and Folders

Some files and folders should not be restored during a restoration. In truth, they should not have been backed up in the first place unless you imaged a disk, but in many cases, people do back them up anyway.

The following are examples of some such files and folders that can be excluded from typical restorations done on a Windows 10 machine. If you're using backup software, the software likely excluded these files when creating the backup. If you are copying files manually, you may have backed them up.

- Contents of the Recycle Bin
- Browser caches (temporary Internet files from web browsers, such as Microsoft Edge or Internet Explorer, Firefox, Chrome, Vivaldi, or Opera)
- Temporary folders (often called Temp or tem and reside in C:\, in the user directory, or in the data directory of software
- Temporary files (usually files named *.tmp or *.temp)
- Operating system swap files (pagefile.sys)
- Operating system hibernation-mode system image information (hyberfil.sys)
- Backups (unless you want to back up your backups) such as Windows File History backup

- Operating system files backed up during an operating system upgrade (usually found in C:\Windows.old on Windows computers that have had their operating systems upgraded)
- Microsoft Outlook cache files (*.ost — note that Outlook local data stores [*.pst] should be backed up; in fact, in many cases they may be the most critical files in a backup)
- Performance log files in directories called PerfLogs
- Junk files that users create as personal temporary files to hold information (for example, a text file in which the user types a phone number that someone dictated to him or her, but which the user has since entered into his or her smartphone directory)

In-app backups

Some applications have built-in backup capabilities that protect you from losing your work if your computer crashes, power fails and you don't have battery power left, and other mishaps.

Some such applications will automatically prompt you to restore documents that would otherwise have been lost due to a system crash or the like. When you start Microsoft Word after an abnormal shutdown of the application, for example, it provides a list of documents that can be autorecovered — sometimes even offering multiple versions of the same document.

Understanding Archives

The term *archive* has multiple meanings in the world of information technology. I describe the relevant meanings in the following sections.

Multiple files stored within one file

Sometimes multiple files can be stored within a single file. This concept was addressed with the concept of virtual drives earlier in this chapter and in Chapter 13. However, storing multiple files within one file does not necessitate the creation of virtual drives.

You may have seen files with the extension .zip, for example. *ZIP files*, as such files are called, are effectively containers that hold one or more compressed files. Storing multiple files in such a container allows for far easier transfer of files (a single ZIP file attached to an email is far easier to manage than 50 small individual files). It also reduces the amount (sometimes significantly) of disk space and Internet bandwidth necessary to store and move the files.

If you need to restore files from an archive, you can either extract all the files from the archive to your primary source, or you can open the archive and copy the individual files to your primary location as you would with any files found in any other folder.

Archive files come in many different formats. Some appear automatically as folders within Windows and Mac file systems and their contents as files and folders within folders. Others require special software to be viewed and extracted from.

Old live data

Sometimes old data is moved off of primary systems and stored elsewhere. Storing old data can improve performance. For example, if a search of all email items means searching through 25 years' worth of messages, the search will take far longer than a search through just the last 3 years. If nearly all relevant results will always be within the last few years, the older emails can be moved to a separate archive where you can access and search them separately if need be.

If you use archiving, factor that in when restoring data. You want to ensure that archives are restored to archives and that you don't accidentally restore archives to the primary data stores.

Old versions of files, folders, or backups

The term *archives* is also sometimes used to refer to old versions of files, folders, and backups even if those files are stored on the primary data store. Someone who has ten versions of a contract, for example, that were executed at different points in time, may keep all the Word versions of these documents in an Archive folder.

Archiving of this sort can be done for any one or more of many reasons. One common rationale is to avoid accidentally using an old version of a document when the current version should be used.

If you're archiving, factor that in when restoring data. Restore all the archives to their proper locations. You may see multiple copies of the same file being restored; don't assume that that is an error.

Restoring Using Backup Tools

Restoring using backup software is similar to the process of backing up using backup software.

To restore using the backup software that was utilized to create the backups from which you are restoring, run the software (in some cases, you may need to install the software onto the machine, rather than run it from a CD or the like) and select Restore.

When you restore, make sure that you select the correct backup version to restore from.

WARNING Beware of bogus restoration prompts! Various forms of malware present bogus prompts advising you that your hard drive has suffered some sort of malfunction and that you must run a restore routing to repair data. Only run restores from software that you obtained from a reliable source and that you know that you can trust!

Many modern backup software packages hide the approach used to back up — full, differential, incremental, and so on — from users and instead allow users to pick which version of files they want to restore.

If you're restoring using the specialized backup and recovery software that came with an external hard drive or solid-state device that you use to back up your device, attach the drive, run the software (unless it runs automatically), and follow the prompt to restore.

Such software is usually simple to use; restoration typically works like a simplified version of that done using other backup software (see preceding section).

REMEMBER Disconnect the drive from the system after performing the restore!

Restoring from a Windows backup

To restore from a Windows backup to the original locations from which the data was backed up, follow these steps:

1. **Choose Start ⇒ Settings ⇒ Update & Security ⇒ Backup.**
2. **Click on Restore files from a current backup.**
3. **In the File System viewer, browse through different versions of your folders and files or type and search for the name of the file you're looking for.**
4. **Select what you want to restore.**
5. **Click on Restore.**

Restoring to a system restore point

Microsoft Windows allows you to restore your system to the way it looked at a specific time at which the system was imaged by the operating system:

1. **Click on the Start button and select Settings.**
2. **Choose Control Panel ⇒ System and Maintenance ⇒ Backup and Restore.**
3. **Click on Restore My Files to restore your files or Restore All Users' Files to restore all users files (assuming that you have permissions to do so).**

Restoring from a smartphone/tablet backup

Many portable devices come equipped with the ability to automatically sync your data to the cloud, which allows you to restore the data to a new device if your device is lost or stolen.

Even devices that do not have such a feature built in almost always can run software that effectively delivers such features for a specific folder tree or drive.

When you start an Android device for the first time after a factory reset, you may be prompted if you want to restore your data. If you are, restoring is pretty straightforward. Answer yes.

While the exact routines may vary between devices and manufacturers, other forms of restore generally follow some flavor of the following process:

To restore contacts from an SD card:

1. **Open the Contacts App.**

   If there is an import feature, select it and jump to Step 4.
2. **Select Settings from the main menu (or click on the Settings icon).**

   If you aren’t displaying all contacts, you may need to click the Display menu and select All Contacts.
3. **Select Import / Export Contacts (or, if that option is not available, select Manage Contacts and then select Import Contacts on the next screen).**
4. **Select Import from SD Card.**
5. **Review the file name for the backup of the Contact list then click on OK.**

   Contacts are often backed up (or exported to) VCF files.

To restore media (pictures, videos, and audio files) from an SD card:

1. **Using File Manager, open the SD card.**

2. **Click to turn on check boxes next to the file or files that you want to restore.**
3. **To copy files to the phone's memory, go to the menu and select Copy ⇒ Internal Storage.**
4. **Select the folder to which you want to copy the files or create the folder and move into it.**
5. **Select Copy Here.**

Restoring from manual file or folder copying backups

To restore from a manual file or folder copy, just copy the file or folder from the backup to the main data store. (If you are overwriting a file or folder, you may receive a warning from the operating system.)

REMEMBER Disconnect the media on which the backup is located from the main store when you are done.

Utilizing third-party backups of data hosted at third parties

If you utilized the backup capabilities of a third-party provider at which you store data in the cloud or whose cloud-based services you utilize, you may be able to restore your relevant data through an interface provided by the third-party provider.

If you use a third-party cloud-based-service provider and you have not performed backups, you may still be able to restore data. Contact your provider. The provider itself may have backed up the data without notifying you.

TIP While you should never rely on your cloud service provider performing backups that you did not order, if you are in a jam and contact the provider, you may (or may not) be pleasantly surprised to find out that they do have backups from which you can restore.

Returning Backups to Their Proper Locations

After you restore from a physical backup, you need to return it to its proper location for several reasons:

- You do not want it to be misplaced if you ever need it again.
- You do not want it to be stolen.
- You want to ensure that you do not undermine any storage strategies and procedures intended to keep backups in different locations than the data stores that they back up.

Network storage

Ideally, when restoring from a network-based backup, you should mount the network drive as read-only to prevent possible corruptions of the backup. Furthermore, be sure to disconnect from the network data store once you are done performing the restoration.

TIP Make sure that whatever mechanism you are using to run the restore (for example, backup software) has the proper network permissions to write to the primary data storage location.

Restoring from a combination of locations

There is no reason to back up to only one location. Restoration, however, typically will utilize backups from only one location at a time.

If you do need to restore from backups that are physically situated at more than one location, be extremely careful not to restore the wrong versions of files as some of the files may exist on multiple backups.

Restoring to Non-Original Locations

When it comes to restoring data, some folks choose to restore to locations other than original locations, test the restored data, and then copy or move it to the original locations. Such a strategy reduces the likelihood of writing over good data with bad data. You can make a bad day worse if you lose some of your data and discover that your backup of the data is corrupted. If you then restore from that backup over your original data and thereby corrupt it, you lose even more of your data.

Never Leave Your Backups Connected

WARNING After restoring, never leave backup hard drives or solid-state drives connected to the systems or networks that they are backing up. Any future malware infections that attack the primary system can spread to the backups as well. Removing your backup from being connected to the material that it is backing up can make all the difference between quickly recovering from a ransomware attack and having to pay an expensive ransom to a criminal.

If you back up to write-once read-many-times media, such as CD-Rs, it is theoretically safe to leave the backup in an attached drive after you finalize the restoration, but you still should not do so. You want the backup to be readily available in its proper location in case you ever need it in the future.

Restoring from Encrypted Backups

Restoring from encrypted backups is essentially the same as restoring from non-encrypted backups except that you need to unlock the backups prior to restoration.

Backups that are protected by a password obviously need the proper password to be entered. Backups protected by certificates or other more advanced forms of encryption may require that a user possess a physical item or digital certificate in order to restore.

In most cases, security conscious home users protect their backups with passwords. If you do so (and you should), do not forget your password.

Testing Backups

Many folks have thought that they had proper backups only to discover when they needed to restore that the backups were corrupted. Hence, testing backups is critical.

While theoretically you should test every backup that you make and test every single item within the backup can be restored, such a scheme is impractical for most people. But do test the first backup that you make with any software, check the auto-recover files the first time that you use Word, and so on.

Some backup software comes with the capability to verify backups — that is, after making a backup, it checks that the original data and data in the backups matches. Running such verification after making a backup adds significant time to the backup process. However, it's well worth running if you can do so because it helps ensure that nothing was improperly recorded or otherwise corrupted during the backup process.

Restoring Cryptocurrency

Restoring cryptocurrency after it is erased from a computer or some other device it was stored on is totally different than any of the restore

processes described in this chapter.

Technically speaking, cryptocurrency is tracked on a ledger, not stored anywhere, so the restoration is not to restore the actual cryptocurrency, but rather to restore the private keys needed in order to control the addresses within the ledger at which the cryptocurrency is stored. (I hate the term *digital wallets* as applied to cryptocurrency — we store digital keys, not cryptocurrency, in a digital wallet. The name *digital keyring* would have been far more accurate and less confusing.)

Hopefully, if you lost the device on which your cryptocurrency is stored, you have the keys printed on paper that is stored in a safe or safe deposit box. Obtain the paper, and you have your keys. Just don't leave the paper lying around; put it back into the secure location ASAP. (If you keep the paper in a safe deposit box, consider performing the restoration technique at the bank so that you never take the paper out of the safe deposit box area.)

If you store cryptocurrency at an exchange, you can restore your credentials to the exchange through whatever means the exchange allows. Ideally, if you properly backed up your passwords to a secure location, you can just obtain and use them.

For those who use hardware wallets to store the keys to their cryptocurrency, the backup for the wallet device is often a *recovery seed*, which is a list of words that allows the device to re-create the keys needed for the relevant addresses. It is generally accepted that the list of words should be written down on paper and stored in a bank vault and/or safe, not stored electronically.

Booting from a Boot Disk

If you ever need to boot from a boot disk that you created (as might be necessary during a system reset and restore process), boot your system, go into the BIOS settings, and set the boot order to start with the disk from which you want to boot. Then restart the system.