SANS OUCH! Newsletter | Got Backups?

Greg Scheidel

5-6 minutes

Overview

If you use a computer or mobile device long enough, sooner or later something will go wrong. You may accidentally delete the wrong files, have a hardware failure, or lose a device. Even worse, malware may infect and wipe or encrypt your files. At times like these, backups are often the only way you can rebuild your digital life.

Backups are copies of your information stored somewhere other than on your computer or mobile device. When you lose, or cannot access, valuable data on your device, you can recover your data from backups. Many of the files we create today are already automatically stored and backed-up in the cloud, such as Microsoft Word documents stored in Microsoft OneDrive, Dropbox, or Google Drive, or personal photos stored in Apple iCloud. But there may be files you create that are not automatically stored in the cloud; or perhaps you want additional backups for personal use.

What, When, and How

The first step is deciding what you want to back up: (1) specific data that is important to you; or (2) everything, perhaps including your entire operating system. Many backup solutions are configured by default to use the first approach and only back up the most commonly used folders. If you are not sure what to back up or want to be extra careful, consider backing up everything.

Second, decide how frequently to back up the data. Built-in backup programs such as Apple’s Time Machine or Windows Backup and Restore allow you to create an automatic “set it and forget it” schedule. Common scheduling options include

hourly, daily, and weekly. Other solutions may offer “continuous protection” in which files are immediately backed up as they are edited or saved. At a minimum, we recommend automated daily backups of critical files.

Finally, decide how you are going to back up. There are two ways: local or cloud-based backups. Local backups rely upon devices you physically control such as external USB drives or network accessible devices. The advantage of local backups is that they enable you to back up and recover large amounts of data quickly. The disadvantage is that if you become infected with malware, it is possible for the infection to spread to your backups. Also, if you have a disaster, such as fire or theft, you could lose your backups as well as your computer. If you use external devices for backups, store a copy offsite in a secure location and make sure your backups are properly labeled. For additional security, consider encrypting your backups.

Cloud-based solutions are online services that back up and store your files on the internet. Typically, you install an application on your computer. The application then automatically backs up your files either on a defined schedule or as you modify or save them. Some advantages of Cloud Solutions are their simplicity, automation of backups, and the access to files from almost anywhere. Also, since your data resides in the cloud, home disasters such as fire or theft will not affect your backup. The main disadvantage is the bandwidth it consumes. Your ability to backup and restore depends on how much data you are backing up and the speed of your network. Not sure if you want to use local or cloud-based backups? Be extra safe and use both.

With mobile devices, most of your data such as emails, text messages, or photos you take are automatically stored in the cloud. However, your mobile app configurations, system preferences, and other files may not be stored in the cloud. By automatically backing up your mobile device, not only do you preserve this information, but it is easier to transfer your data when you upgrade to a new device.

Additional Key Points

- Regularly test that your backups are working by retrieving and opening a file.
- If you rebuild a system from backup including the operating system, be sure you reapply the latest security patches and updates before using it again.

- If you are using a cloud solution, select one that is easy for you to use and research the security options. For example, does your cloud backup vendor support two-step verification to secure your online account?

Backups are a simple and low-cost way to protect your digital life.

Guest Editor

Greg Scheidel is the Chief Cybersecurity Officer at Iron Vine Security, with over 30 years IT and IT security experience. He is also a SANS instructor, teaching security architecture, engineering, and zero trust in SEC530. You can reach him on Twitter @greg_scheidel.

***** Resources**

Two-Factor Authentication: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

Securely Using the Cloud: https://www.sans.org/newsletters/ouch/securely-using-the-cloud/

Password Manager: https://www.sans.org/newsletters/ouch/password-managers/

Digital Inheritance: https://www.sans.org/newsletters/ouch/digitalinheritance/

Reprinted from: https://www.sans.org/newsletters/ouch/backups/