Got Backups?

Overview

If you use a computer or mobile device long enough, something will eventually go wrong. You may accidentally delete the wrong files, have a hardware failure, or lose a device. Even worse, malware, such as ransomware, may wipe your files and/or hold them captive. At times like these, backups are often the only way you can rebuild your digital life.

What, When, and How

Backups are copies of your information stored somewhere other than on your computer or mobile device. When you lose valuable data, you can recover your data from backups. The first step is deciding what you want to back up: specific data that is important to you or everything, including your entire operating system. Many backup solutions are configured by default to use the first approach. They back up the most commonly used folders. If you are not sure what to back up or want to be extra careful, back up everything.

Second, decide how frequently to back up. 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 options include hourly, daily, weekly, etc. Other solutions offer "continuous protection" in which new or altered files back up immediately each time you save a document. At a minimum, we recommend automated daily backups of critical files.

Finally, decide how you are going to back up. There are two ways: locally or Cloud-based. Local backups rely upon devices you control, such as external USB drives or Wi-Fi accessible network devices. The advantage of local backups is that they enable you to back up and recover large amounts of data quickly. The disadvantage is if you become infected with malware, such as Ransomware, it is possible for the infection to spread to your backups. Also, if there's a fire, theft, or other disaster, it can result in you losing not only your computer, but the backups, as well. If you use external devices for backups, store a copy off-site in a secure location and make sure your backups are properly labeled.

Cloud-based solutions are online services that store your files on the Internet. Typically, you install an application on your computer. The application then automatically backs your files either on a schedule or as you modify them. An advantage of Cloud solutions is their simplicity; backups are often automatic, and you can usually access your files from anywhere. Also,

since your data resides in the Cloud, home disasters, such as fire or theft, will not affect your backup. Finally, Cloud backups can help you recover from malware infections such as Ransomware. The disadvantage is your ability to back up and restore depends on how much data you have backed up and the speed of your network. Not sure if you want to use local or Cloud-based for backups? Be extra safe and use both.

With mobile devices, most of your data is already stored in the Cloud. However, your mobile app configurations, recent photos, and system preferences may not be. By 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.

Key Points

- **Backing up your data is only half the battle. You must also be sure that you can recover it. Test periodically that your backups are working by retrieving and opening a file.**
- **If you rebuild a system from a backup, 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, do they support two-step verification to secure your online account?**

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

Subscribe to OUCH! and receive the latest security tips in your email every month - sans.org/ouch.
Do you think you've got what it takes to get into the cyber security industry? Or are you looking to improve your existing skillset? Training with SANS helps you achieve your goals. Level Up with SANS today! sans.org/Level-Up-Ouch

Guest Editor

Matt Bromiley *is a cybersecurity professional and incident responder who has worked with organizations of all sizes. He is also a SANS instructor, and teaches FOR508 - Advanced Host and Network Incident Response and FOR572 - Threat Hunting. You can reach him on Twitter @mbromileyDFIR.*

Resources

Making Passwords Simple:	https://www.sans.org/u/TqR
Stop That Malware:	https://www.sans.org/u/TqW
Creating a Cybersecure Home:	https://www.sans.org/u/Tr1