The Monthly Security Awareness Newsletter for Everyone

OUCH!

IN THIS ISSUE...

- Backups: What, When, and How
- Recovery
- Key Points

Backup & Recovery

Overview

If you use a computer or mobile device long enough, sooner or later something will go wrong, resulting in you losing your personal files, documents, or photos. For example, you may accidently delete the wrong files, have a hardware failure, lose a device, or become infected with malware, such as ransomware. At times like these, backups are often the only way you can rebuild your digital life. In this newsletter, we explain what backups are, how to back up your data, and how to develop a simple strategy that's right for you.

Guest Editor

Keith Palmgren is a cybersecurity professional with over 30 years of experience in the IT Security field. He is a SANS Senior Instructor and the author of SANS SEC301: Introduction to Information Security. Keith runs a successful security consulting practice and is on Twitter: **@kpalmgren**.

Backups: What, When, and How

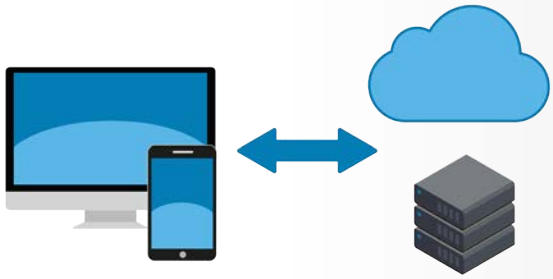
Backups are copies of your information stored somewhere other than on your computer or mobile device. When you lose valuable data, you can recover that data from your backups. Unfortunately, too many people fail to perform regular backups, even though they are simple and inexpensive. The first step is deciding what you want to back up. There are two approaches: (1) backing up specific data that is important to you; or (2) backing up everything, including your entire operating system. Many backup solutions are configured by default to use the first approach. They back up data from the most commonly used folders. In many cases, this is all you need. However, if you are not sure what to back up or want to be extra careful, back up everything.

Second, you must decide how frequently to back up. Built-in backup programs, such as Apple's Time Machine or Microsoft Windows Backup and Restore, allow you to create an automatic, "set it and forget it" backup 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.

Finally, you need to decide how you are going to back up. There are two ways to back up your data: physical media or Cloud-based storage. Each approach has advantages and disadvantages. If you are not sure which approach to

Backup & Recovery

use, you can use both at the same time. Physical media is devices you control, such as external USB drives or Wi-Fi accessible network devices. The advantage of using your own physical media is it enables you to back up and recover large amounts of data very quickly. The disadvantage of such an approach is if you become infected with malware, such as ransomware, it is possible for the infection to spread to your backups. Also, if you have a disaster, such as fire or theft, it can result in you losing not only your computer, but the backups as well. As such, if you use external devices for backups, you should store a copy of your backup off-site in a secure location. Make sure backups you store off-site are properly labeled.



Automated, reliable backups are often your last line of defense in protecting your data.

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, as many Cloud solutions allow you to recover from pre-infected versions. The disadvantages are it can take a long time to back up or recover very large amounts of data. Also, privacy and security is important. Does the backup service provide strong security controls, such as encrypting your data and two-step verification?

Finally, don't forget your mobile devices. With mobile devices, most of your data, such as email, calendar events, and contacts, is already stored in the Cloud. However, your mobile app configurations, recent photos, and system preferences may not be stored in the Cloud. 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. An iPhone/iPad can back up automatically to Apple's iCloud. Android, or other mobile devices depend on the manufacturer or servicer provider. In some cases, you may have to purchase a mobile app designed specifically for backups.

Recovery

Backing up your data is only half the battle; you must be sure that you can recover it. Check periodically that your backups are working by retrieving a file and making sure it is the same as the original. Also, be sure to make a full system

Backup & Recovery

backup before a major upgrade (such as moving to a new computer or mobile device) or a major repair (like replacing a hard drive) and verify that it is restorable.

Key Points

- Regardless of what solution you use to back up your data, make sure you automate your backups and check them periodically.
- When rebuilding a system from backup, be sure you reapply the latest security patches and updates before using it again.
- Outdated backups that are no longer needed are a liability; destroy them to prevent access by unauthorized individuals.
- If you are using a Cloud solution, research the policies and reputation of the provider and make sure they meet your requirements. For example, do they encrypt your data? Do they support strong authentication, such as two-step verification?

2017 Security Awareness Report

It's here! Get your copy of the 2017 SANS Security Awareness report, *It's Time to Communicate*. It's jam-packed with data on security awareness, giving you tips and tricks to keep you safe. Download your free copy: https://securingthehuman.sans.org/resources/security-awareness-report-2017.

Resources

Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Two-Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Cloud Security:	https://securingthehuman.sans.org/ouch/2016#november2016
Encryption:	https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016

License