The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- What To Backup and When
- How To Backup
- Recovery
- Key Points

Personal Backup and Recovery

Overview

Backups are one of the most important steps you can take to protect your information. They allow you to recover your data when something goes wrong, such as hard drive failures, accidental file deletions, stolen or lost devices, or malware infections. In this issue we focus on ways that you can backup up your data and develop a strategy that's right for you.

Guest Editor

Dr. Eric Cole is the guest editor for this issue of OUCH! and is an industry-recognized security expert. He is the author of several books, including Advanced Persistent Threat, Hackers Beware, and Network Security Bible. Dr. Cole is also the founder of Secure Anchor Consulting, a SANS faculty Fellow and course author. Learn more at at www.securityhaven.com or Twitter: @drericcole.

What To Backup and When

There are two basic approaches on deciding what to back up: (1) specific data that is important to you, such as documents, pictures, or videos; or (2) everything, including your operating system and any programs you have installed in addition to your unique data. The first approach streamlines your backup process, however the second approach is simpler and more reliable if you have to recover from a complete system failure. If you are not sure what to back up, then back up everything.

Your next decision will be deciding how frequently to backup your data. Common options include hourly, daily, weekly, etc. For home use, personal backup programs such as Apple's Time Machine or Microsoft's Windows Backup and Restore allow you to create a simple and automatic "set it and forget it" backup schedule. These solutions will silently back up your data while you are working on or away from your computer. Other solutions offer "continuous protection" in which new or altered files are immediately backed up as soon as they're closed.

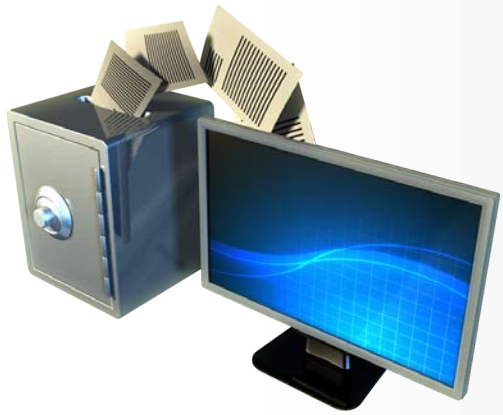
How To Backup

In general there are two ways to backup your data: physical media or cloud-based storage. Physical media includes DVDs, USB drives, or external hard drives. When using physical backups make sure you are not backing up your files to the same device that holds the original files. Also, be sure to label your media externally so that you can easily identify a backup from a particular date and time. The advantage with physical media

© The SANS Institute 2013

Personal Backup and Recovery

is backups, and recovery, are much faster. The disadvantage is if your location has a disaster (such as a fire) then not only can you lose your computer but the backups as well. As such you should have a plan to store copies of your backup off-site. When storing backups off-site, consider encrypting the backups - that way if they are lost or stolen your data is still protected. If you do encrypt your backups, be sure you securely store the passwords so you do not lose or forget them over time.



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

Cloud based solutions are different, this is service where your files are stored in the Cloud (somewhere on the Internet). Depending on how much data you want to backup, this may be a paid service. It works by installing a program on your computer which then automatically backups up your files for you. The advantage with this solution is you do not have to worry about the file storage, everything is taken care of you. The disadvantage is Cloud based backups (and recovery) can be much slower, especially if you have a large amount of data.

Don't forget to backup your mobile devices also. While most of the data on your mobile device is already stored in the Cloud, such as your email or calendar events, some of the data on your mobile device is unique, such as recent photos or videos you may have taken. Your iPhone/iPad can backup to any computer which has iTunes installed or to Apple's iCloud. For Android or other types of mobile devices, backup options depend on the manufacturer or servicer provider. In some cases you may have to purchase mobile apps designed specifically for backups.

Recovery

Backing up your data is only half the battle; you have to be certain that you can recover it. Check every month that your backup program is working. If nothing else, try recovering a file and verify its contents. In addition, be sure to make a full system backup before a major upgrade (such as moving to a new computer) or a major repair (like replacing a hard drive) and verify that it is restorable.

© The SANS Institute 2013

Personal Backup and Recovery

Key Points

- Automate your backup process as much as possible, but verify that it runs correctly.
- When rebuilding an entire system from backup, be sure you reapply the latest security patches and updates before putting it back into service.
- Outdated or obsolete backups may become a liability, and should be destroyed in order to prevent them being accessed by unauthorized users.
- If you are using a cloud solution, research the policies and reputation of the organization and make sure they meet your requirements. For example, do they encrypt your data when it is stored? Who has access to your backups? Do they support strong authentication?
- When possible, the most reliable method to backing up your data may be a combination of both physical media and cloud services.

SANS Network Security 2013

Join SANS Institute, the world's most trusted source for computer security training, in Las Vegas September 14 - 23 for Network Security 2013! Choose from more than 45 hands-on courses from beginner to advanced levels in IT security, pen testing, forensics, audit, management , and ICS/SCADA. Learn more at http://www.sans.org/info/136317.

Resources

Apple Time Machine:	https://support.apple.com/kb/ht1427
Windows 7 Backup and Restore:	http://windows.microsoft.com/en-US/windows7/products/features/backup-and-restore
Cloud Backup:	http://open-tube.com/what-is-cloud-backup-a-beginners-guide-to-cloud-backup/
Cloud Backup Services:	http://online-backup-services-review.toptenreviews.com/
Backup Apps for Android:	http://arstechnica.com/gadgets/2013/04/better-safe-than-sorry-five-backup-apps-to-consider-for-your-android-device/

OUCH! is published by SANS Securing The Human and is distributed under the Creative Commons BY-NC-ND 3.0 license.
You are free to distribute this newsletter or use it in your awareness program as long as you do not modify the newsletter.
For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis