Protecting & Sharing Your Data

Tim Hannon

tim@soundsupport.biz
www.soundsupport.biz

October 26, 2013

SOUND SUPPORT

Macintosh Support, Training and Consulting

Today's Topics

Protecting and Sharing Your Data

1. Smart Backup Strategies

2. Strong Passwords

3. Online (Cloud) File Sharing Systems

You can download a PDF copy of today's presentation at:

http://www.soundsupport.biz/red-pencil

SOUND SUPPORT

Why Back Up?

Topic 1 of 3

1. There are two kinds of people in this world. Those who have lost data and those who will lose data.

2. If it's worth backing up once, then it's worth backing up twice.

SOUND SUPPORT

Poll The Audience

1. Who has lost data?

2. Who backs up their computer?

SOUND
SUPPORT

Reasons To Back Up

1. You might want a **previous version** of a document.

2. Your **files** can get **damaged.** Damaged files may not open and thus data can be lost.

3. You can accidentally **delete** or over-write a **file.**

4. Your **hard drive** might **fail.** All drives will fail eventually on their own, or possibly immediately if they are dropped.

5. Your computer could be damaged by **fire**, **flood** or **burglary.** It's rare, but it happens.

SOUND
SUPPORT

Friday, October 25, 13

Backup Requirements

A comprehensive back up system should do the following:

1. Copy all files (operating system, applications and your personal data)

2. Run frequently and automatically

3. Produce multiple files, stored on multiple drives, kept in multiple locations

- *Dropbox* (or other file sharing systems) do not offer the same amount of protection as a robust backup application.

- Back up your smartphone and/or tablet to your computer

6

SOUND SUPPORT

3-2-1 Backup Rule

	Main Copy on Computer	Backup Copy 1	Backup Copy 2
3 Copies	Main Copy on Computer	Backup Copy 1	Backup Copy 2
2 Media		External Hard Drive	Cloud Storage or HD at Friend's
1 Off-site			Cloud Storage or HD at Friend's
Protection	None	Low	High

SOUND SUPPORT

Friday, October 25, 13

3-2-1 Backup Systems

Mac OS X–Use ***Time Machine*** with an online backup service like ***CrashPlan.*** *Time Machine requires OS X 10.5 or newer. CrashPlan free or $60/yr*

Windows 7–Use **Backup and Restore** with an online backup service like ***CrashPlan.***

Windows 8–Use **File History**, Acronis' ***True Image*** ($50) and an online backup service like ***CrashPlan***.

See Resources for articles about setting up Mac and Windows backups.

SOUND
SUPPORT

Friday, October 25, 13

Cost Comparison

Backup System	No Backup System
External Hard Drive ~$125	*DriveSavers* Professional Data Recovery, starts at $500
Annual Subscription to *CrashPlan* ~$60	Typical costs ~$1500-$2500 plus pain and suffering
Acronis *True Image* ~$50	Expedited service costs more
Downtime is minutes or hours, maybe a day or two at most	Downtime is measured in days or weeks

SOUND SUPPORT

Strong Passwords

Topic 2 of 3

1. Security and convenience are currently inversely related.

2. Security today is typically tied to passwords.

3. We need to strike the best balance between the security of long, complex passwords and the convenience of memorable passwords

SOUND SUPPORT

Poll The Audience

1. Who has had one of their online accounts broken into? (Gmail, Yahoo, eBay, etc.)

2. Who has had a computer, tablet or smartphone lost or stolen?

SOUND SUPPORT

Selecting Passwords

Recommendations

1. Make them **long** and **memorable**. Every extra character makes the password exponentially stronger.

2. Use a **minimum** of **10** characters–a **mix** of letters, numbers, and symbols.

3. Test a password's strength using Mac OS X's *Password Assistant* or one of the websites listed in *Resources*.

Examples

2%MilkHasLessFat (16 characters)

$200HaircutsAreExpensive (24 characters)

Andrew'sBirthdayIs10/26/78 (26 characters)

SOUND SUPPORT

Storing Passwords

3 Options

1. **Paper**–Write a hint, not the password itself.

2. **Computer File**–Store a Word or Excel file in an encrypted disk image. Create an encrypted disk image using OS X's *Disk Utility*, *TrueCrypt* (free Mac and PC) or *BoxCryptor*.

3. **Password Manager Applications**

   - *1Password* (Mac, Windows, iOS, Android)

   - *KeePass* (Free, PC-only)

   - *LastPass* (Web-based)

See Resources for articles disk images and password managers

SOUND SUPPORT

Online File Sharing

Topic 3 of 3

1. Compare popular file sharing systems

2. Assess risks of file sharing systems

3. Recommendations to handle risks

SOUND SUPPORT

Poll The Audience

1. Who uses an online file sharing system, such as Dropbox, SkyDrive, or GoogleDrive?

2. Why do you use it?

SOUND
SUPPORT

Comparing Basics

Company	Inception	Free Storage	Entry Paid Plan	Max File Size	File Versioning
Dropbox	**2007**	2 GB	$100/yr 100 GB	Unlimited	Yes, free acct only 1 mn of ver.
Google Drive	2012	**15 GB**	$60/yr 60 GB	10 GB	Yes
SkyDrive	2007	7 GB	**$10/yr 32 GB**	2 GB	Yes
Box (Box.net)	2007	10 GB	$60/yr 100 GB	5 GB paid, **250 MB free**	**Only with paid accounts**
SugarSync	2008	30 days only	$75/yr 60 GB	Unlimited	Yes, last 5 versions
Hightail (YouSendIt)	2004	2 GB	$160/yr unlim.	2 GB paid, **50 MB free**	Yes

SOUND
SUPPORT

Distinguishing Features

- Dropbox seems to have the most **3rd-party apps.** (1Password, Notability, etc.)

- GoogleDrive and SkyDrive support **collaborative editing.**

- Google Drive and SkyDrive do **not** support Blackberry phones.

- GoogleDrive does **not** support Windows Phones.

SOUND SUPPORT

Cloud Sharing Risks & Considerations

- Does the company back up your data and will they restore all of it?

- Who has access to your data? Hosting company, our government, foreign governments, everybody?

Examples

1. Gmail account hacked. All data deleted only 10% initially restored from backup.

2. Dropbox security breach. Any password could be used to access any Dropbox account.

3. Most companies have a master password which they can use to get into your account.

See Resources for citations on these 3 examples

SOUND SUPPORT

Strategic Solutions

Recommendations

- Have a local backup of data you store in the cloud.

- Pick strong account passwords.

- Encrypt files that you store in online file sharing systems using **BoxCryptor**.

- Use a second password to secure data. **CrashPlan** lets you set a second password called an *archive* password.

See Resources for articles about Boxcryptor and archive password in CrashPlan.

SOUND SUPPORT

Key Takeaways

Recommendations to Protect and Share Your Data

❖ Setup a robust, automatic backup system with both on-site and off-site copies. (Use the 3-2-1 model.)

❖ Strengthen your passwords using long phrases of words, numbers, and symbols.

❖ If you use cloud backup or file sharing systems, don't blindly rely on them. Be responsible for backing up your own data, use a strong account password and protect some or all files with a second level of password protection.

SOUND SUPPORT

Questions

Tim Hannon

tim@soundsupport.biz

www.soundsupport.biz

SOUND
SUPPORT

		Resources for Protecting & Sharing Your Data	
		Red Pencil Presentation Oct 26, 2013	
Slide 8	3-2-1 Backup Sys	Time Machine Overview and Setup	http://www.soundsupport.biz/2011/01/30/how-to-setup-and-monitor-time-machine/
		Time Machine With Multiple Drives	http://www.soundsupport.biz/2010/09/05/setting-up-time-machine-to-use-multiple-hard-drives/
		Take Control of Easy Mac Backups	https://www.takecontrolbooks.com/backup-easy-mac-old?pt=TB-ARTICLE-10909
	Windows 7 Backup	Backup and Restore Overview	http://www.pcworld.com/article/186997/win7_backup.html
		Backup and Restore Strategies	http://www.pcworld.com/article/170688/7_backup_strategies_for_your_data_multimedia_and_system_files.html
		Backup and Restore Setup Instruc.	http://www.makeuseof.com/tag/set-windows-7-backup-restore-feature/
	Windows 8 Backup	File History	http://www.makeuseof.com/tag/did-you-know-windows-8-has-a-built-in-time-machine-backup/
Slide 12	Selecting Passwords	Test Password Strength	http://www.soundsupport.biz/2012/04/01/how-secure-is-your-password/
		Apple Password Assistant	http://www.macworld.com/article/1145804/passwordassistant.html
Slide 13	Storing Passwords	Create Encrypted Disk Image on Mac	http://www.soundsupport.biz/2010/02/14/how-to-create-and-use-an-encrypted-disk-image/
		Encrypt USB flash drive	http://www.makeuseof.com/tag/encrypt-your-usb-stick-with-truecrypt-60/
		1Password ver 4 Review	http://tidbits.com/article/14138
		Take Control of 1Password	http://www.takecontrolbooks.com/1password?pt=TB1194
Slide 18	Cloud Risks	Dropbox Security Risks	http://money.cnn.com/2011/06/22/technology/dropbox_passwords/index.htm

		General complaints	http://blogs.cio.com/cloud-computing/17574/dirty-secrets-dropbox-google-drive-and-other-cloud-storage-services
		How to Tell If Your Cloud Provider Can Read Your Data	http://tidbits.com/article/12920
		GMail account hacked	http://www.theatlantic.com/magazine/archive/2011/11/hacked/308673/
		Backup Google Acct with CloudPull (Mac only)	http://www.goldenhillsoftware.com
		CloudPull Review	http://tidbits.com/article/12840
Slide 19	Recommendations	5 Ways to Encrypt Files in Cloud	http://www.makeuseof.com/tag/5-ways-to-securely-encrypt-your-files-in-the-cloud/
		Boxcryptor to secure Dropbox files	http://www.makeuseof.com/tag/encrypt-dropbox-files-boxcryptor/
		Protect your CrashPlan data with 2nd password	http://support.crashplan.com/doku.php/faq/security#what_s_the_difference_between_an_account_password_and_an_archive_password