April 2013
Vol. XXIV, No 4

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ http://www.keystonemac.com

KEYMAC ANNUAL AUCTION

Keystone MacCentral is having its annual auction on Tuesday April 16th upstairs at the Camp Hill Giant. The auction is open to both members and non-members so bring a friend.

Thanks to Eric Adams who does most of the leg work, we will again have a great list of vendors participating this year. That means great software and hardware for you to bid on and great values. A great deal of thanks goes to the vendors who have been very supportive of users groups like ours.

The auction will start promptly at 6:30 and must end by 9:00 pm. With that in mind, we will have to limit club members' auction items to 5. Bring in good stuff — it should run OS X 10. Sellers will make 80% of the highest bid with the remaining 20% going to the club. Pick up an auction ID card when you arrive.

We do have a few rules.

An Auction Form must be filled out and attached to each separate item to be auctioned. Keep the description brief (there's not much room) and readable, BUT include enough information to make your article attractive. Use the back of the form, if necessary. Copies will be available at the auction.

On the Auction Form, the Seller # is your membership number, which can be found on the auction ID card issued at the begging of the meeting. Non-members can obtain a Seller # during registration before the auction. If you have a minimum acceptable bid, include that amount in the Min Bid box.

Bids will be taken in minimum of $1 increments only. Payment must be made in cash. Checks will be accepted from Keystone MacCentral members only.

Keystone MacCentral does not assume any liability for any product bought or sold. Disputes about purchased items will need to be resolved between the buyer and seller. We will provide contact information if requested.

Meet us at

Giant Food

Corner of Trindle Road & 32nd St (Route 15)
3301 East Trindle Road, Camp Hill, PA 17011

Tuesday, April 16 2013 6:30 p.m.

Attendance is free and open to all interested persons.

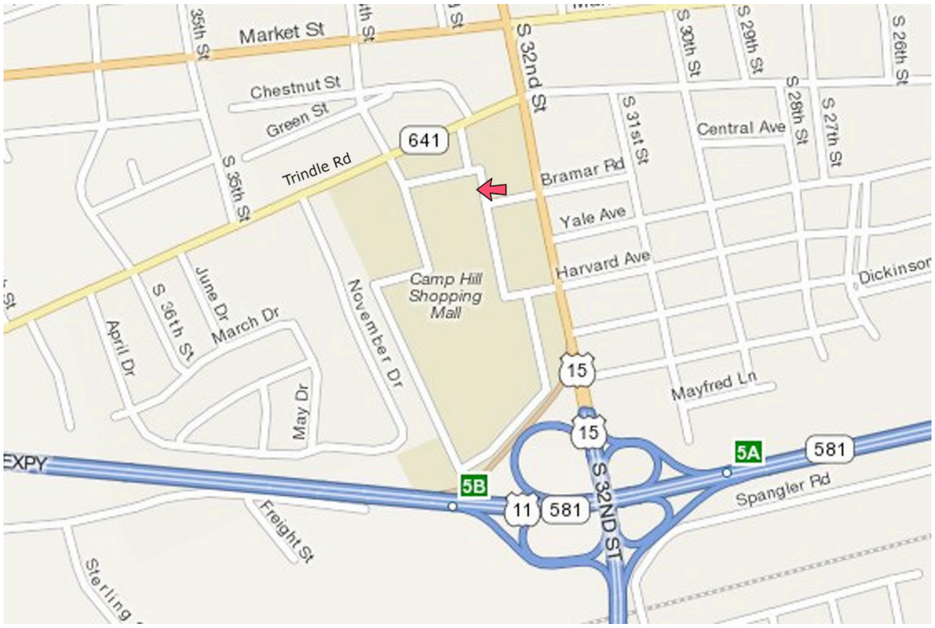
Contents

Keystone MacCentral is a not-for-profit group of Macintosh enthusiasts who generally meet the third Tuesday of every month to exchange information, participate in question-and-answer sessions, view product demonstrations, and obtain resource materials that will help them get the most out of their computer systems. Meetings are free and open to the public. The *Keystone MacCentral printout* is the official newsletter of Keystone MacCentral and an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by any for-profit organization, including Apple Inc. Copyright © 2013, Keystone MacCentral, 310 Somerset Drive, Shiresmanstown, PA 17011.

Nonprofit user groups may reproduce articles form the Printout only if the copyright notice is included, the articles have not been edited, are clearly attributed to the original author and to the Keystone MacCentral Printout, and a copy of the publication is mailed to the editor of this newsletter.

The opinions, statements, positions, and views stated herein are those of the author(s) or publisher and are not intended to be the opinions, statements, positions, or views of Apple Computer, Inc.

Throughout this publication, trademarked names are used. Rather than include a trademark symbol in every occurrence of a trademarked name, we are using the trademarked names only for editorial purposes and to the benefit of the trademark owner with no intent of trademark infringement.



Keystone MacCentral Essentials

Meeting Place
Giant Food (upstairs)
Corner of Trindle Road & 32nd St
(Route 15)
Camp Hill

Web Site
http://www.keystonemac.com

Mailing Address
310 Somerset Drive
Shiresmanstown, PA 17011

by Gary Brandt, Recorder

Keystone MacCentral Minutes

March 19, 2013

Business Meeting

President Linda Cober welcomed members and guests to the March meeting. She asked board members to give their reports. Eric Adams said we had begun receiving donations for the auction to be held in April. Items are posted to our web site as we get them. Linda reminded members that they can bring in newer items to sell at the auction on an 80/20 basis, with the club receiving 20% of the sale price.

Q&A & Comments

Someone asked if there was an Apple Learning Camp for adult learning. Apple Stores have different classes at each location, based on who is there to teach them. Best Buy stores have basic training classes. The lynda.com web site has Mac training videos. You can get a 10 day free trial offer if you follow the link to lynda.com from the photofocus.com web site.

A question about Automator actions was posed. That could be a topic for a future program. Someone mentioned the AirRadar for Mac app used to detect locations with WiFi signals.

Jim Carey showed us the kelbytraining.com web site which hosts tutorials on photography. Linda Cober brought in a friend's Mac with a non-working iSight camera. No one in attendance had encountered that problem with their Macs.

Program Notes

Before Jim Carey began his program on Myths and Misconceptions of the Law for Photographers, he showed us a time lapse video taken at a recent meeting of the Hershey Camera Club. It was made with an iPhone and an app called Lapse It.

Laws governing photography in public places have changed since the 9/11/01 terrorist attacks. There still remain gray areas in interpretation of some of these new laws. Jim's Keynote presentation began with a disclaimer that he was not offering legal advice since he is not a lawyer. The presentation posed questions in a true or false format, with the audience giving their answers before additional information on each topic was presented.

News publications can not use your photograph without your permission because that is not considered fair use. Ultimately it is up to the courts to decide fair use issues.

The idea that a model release is needed to use someone's photo on a book cover is not clearly defined by the courts. Each state's laws determine what is required for such use, with New York state said to have the strictest standards. Both model and property releases come into play. A stock photo agency may require a model or property release. A property release covers photos of private property. Newer buildings can be copyrighted.

There are instances when you feel you do not need a model release, but it is always a good idea to get one. A release can be on paper or as an electronic model release that is digitally signed. Be aware that digital editing of electronic documents or Photoshop manipulation of images could present problems. For this reason, a written model release is much preferred.

Legal questions arise if you make money from a print as to whether that is considered commercial use. The courts have ruled that some use is considered to be "fine art" with no compensation required. Mass production of prints is a factor in determining commercial use. In general you can use a photo of a property for commercial use without a property release, if that photo was taken from a public area. Jim gave an example. You can take photos of Hershey Park from public property outside of the park, but once inside the park, you are not permitted to take photos for later commercial use. Jim explained that most venues operate with similar rules.

You do have copyright protection for photos you take before you register them. Registration will enhance your rights. The law is similar for artwork. Copyright infringement is a federal offense that is dealt with only in the federal court system, where an intellectual rights attorney is needed for your case.

Another question related to copyrights comes up when you take a photo while working. The owner of the copyright could be you or your employer, depending on your job description. Most professional photographers attempt to keep all rights to their photos. A well known myth says that if you seal a photograph in an envelope and mail it to yourself you will be copyrighting that photo, but that is not true.

You might think that statues and other works of art on federal or state property are in the public domain. This is mostly true, except for government works exceptions. If your photograph of items in the public domain does not add a creative element, then your photo is also considered to be in the public domain.

Distinctions are made between editorial use and commercial use of a photo, with most editorial use approved.

If you go through copyright registration for your photos, you will be asked if you have published your photo. Items in public view, physically or online, are considered to have been published. Items can also be published with a creative commons license, which allows anyone to use your photos without permission.

The ACLU web site has a section on photographer's rights. Police officers may not generally confiscate or demand to see your photos or videos without a warrant, although the courts have not issued final rulings on such seizures. They are not allowed to delete photos or videos under any circumstance. The Department of Homeland Security is said to have declared a "Constitution-Free Zone" within 100 miles of U.S. borders which could limit your rights in those areas.

For local railroad buffs, Jim related that Norfolk Southern is very strict about photography. Private property owners control your photography when you are on their property. If you are stopped when taking photos, it is best to be polite and never to physically resist. You should ask if you are free to go. If a police officer says you are being detained, he should have reasonable suspicion to detain you.

Jim recommended some web sites: www.thecopyrightzone.com, www.photoattorney.com - www.krages.com, and some reading material: *Photographer's Legal Guide by Carolyn E. Wright, Esq. and Legal Handbook For Photographers* by Bert Krages.

Jim was able to use some clips and other material in his presentation under educational fair use doctrine, since he does not charge anyone to see his presentation. He included the appropriate acknowledgement of sources.

If you are going to submit photographs or video clips to the media, you should first read their Terms of Service. You are basically giving them the rights to use your media. Jim went to the www.copyright.gov web site to show us the electronic copyright process. It takes around six to nine weeks to have copyrights registered. For a fee of $35, you can upload a group of photos (700 x 700 JPEGS) or other artwork. You have only 30 minutes to upload one group. They do accept Zip files. Registration only covers U.S. copyright protection, although the U.S. belongs to a consortium with other countries respecting each other's copyright laws. Fees should be paid by credit card. Everything produced from an original photograph is considered to be derivative and covered by the original photo's copyright.

For a fee of $760 you can go to the Copyright Office to immediately register one item. Canada has recently updated their copyright laws which allow you to copyright one item at a time for about $50.

Jim distributed a handout at the end of the meeting that covered your rights when stopped or confronted for photography. He might have more if you could not attend the March meeting.

I will add my own disclaimer. The above written description of Jim Carey's presentation and topics covered therein should not be considered to be legal advice. Seek the advice of an attorney for your needs.

by Glenn Fleishman

Apple Implements Two-Factor Authentication for Apple IDs

Apple quietly added optional two-factor authentication for Apple ID accounts last week, joining the likes of Google, Dropbox, PayPal, Facebook, and an ever-growing number of other sites. This additional layer of authentication helps protect the increasingly important Apple ID accounts that millions of Mac and iOS users rely on for iTunes Store and App Store purchases, iCloud logins and data sharing, support from Apple, and more.

Although it's optional, we recommend enabling two-factor authentication as soon as is practical for you. Since online criminals can use compromised Apple ID accounts both to siphon money from credit cards and to take over your digital identity, it's no longer paranoid to worry about your password being stolen. Although it may seem like a hassle, and setup should be done with care, Apple's two-factor authentication will not impact your life significantly. Apple says there are only three situations in which two-factor authentication will be invoked:

- When you sign in to the My Apple ID site to manage your account.

- When you make a purchase from the iTunes Store, App Store, or iBookstore from a new device.

- When you get Apple ID-related support from Apple.

Factoring the Security Equation — The "factors" in two-factor authentication refer to two distinct private elements one must know or have to perform a successful login. The first factor is typically a password, as it still is with Apple IDs. The second is an "out-of-band" element: a code that can only be known or created using separately provided hardware or separately registered software. The out-of-band part is important to ensure that someone who already knows your password or has gained access to your computer cannot also obtain the second factor through the same medium.

Two-factor authentication used to be wonky, but with the rise in online crime, we're seeing increasingly widespread support. I have two separate keyfobs, one for PayPal/eBay and another for E*Trade, from which I have to enter a six-digit number whenever I log in to those services. That number changes every minute. Google offers Google Authenticator, a mobile app for iOS, Android, and BlackBerry that can provide the same sort of code more conveniently, once you've associated it with your Google account. Dropbox can use Google Authenticator, too, which is handy, relying on a separately registered and generated entry in the app. Even Facebook offers two-factor authentication through both SMS text messages and the Facebook iOS app. Many other services without apps also rely on SMS text messages to send a code to a mobile device under your control in order to provide the out-of-band component.

This two-factor method replaces the "security questions" that Apple has long relied on, much like many other companies. These questions are typically drawn from a list of possibilities like, "Who was your best friend in school?" But the questions may be ambiguous and can often be hacked easily by identity thieves hoovering up your personal details by searching Google, Facebook, or other personal information services. (In "Take Control of Your Passwords," Joe Kissell recommends coming up with what is essentially a passphrase – not a truthful answer – for each security question.)

Worse, as Mat Honan amply documented when his own accounts were hijacked, crackers can sometimes take over an account using a combination of social engineering and logical failures in password-reset procedures. At one point, Amazon allowed you to add an e-mail address by phone if you had the last four digits of a credit card on file. However, you could also add a credit card by phone. Crackers realized they could add the credit card in one call, hang up, and then call back to add an e-mail address they owned using the stolen (but still active) or faked (but validly formulated) card number they'd just provided. They could then get a password-reset message sent to their e-mail address.

Honan documented that with an Amazon account, an attacker could then view the last four digits of other stored credit card numbers for that account, and use that information to reset passwords or add e-mail addresses to an Apple ID or accounts at other sites.

These attacks fail when the miscreant must both reset the password and either have physical possession of an unlocked device owned by the target or intercept SMS messages bound for that person. For sophisticated attacks targeted at an individual – say someone involved in government or corporate espionage or even a particularly messy divorce – two-factor authentication may still not be enough, but it's more than sufficient to prevent the commonplace drive-by assaults on one's identity.

Factor Your Decision — Before you set up Apple's two-factor authentication, consider what the future looks like after the switch, as there are pluses and minuses with the new method.

On the upside, consider:

- No thief with your password alone can change your password, have Apple make account changes by phone, or gain access to your account to make iTunes Store, App Store, or iBookstore purchases from a new device.

- No more security questions to answer and remember!

- You can reset your password securely (using a linked device and a special recovery key described below) if you forget it or believe it was compromised.

But there are a few downsides, too:

- You must be able to receive SMS messages, or be set up with notifications via Find My iPhone on a particular iOS device. (Apple's assumption appears to be that both reception of SMS messages and Find My iPhone require physical possession of a specific piece of hardware, whereas messages sent via iMessage, for instance, could appear on multiple devices.)

- You can permanently lose access to your account in a particularly complicated scenario that's unlikely, but possible. As Apple describes in a support note, you can reset access to an account as long as you have two of the following: the account password, access to a "trusted" device associated with the account, and a special recovery key generated when you set up two-factor authentication that's used as a last resort. But if you have only one or none of those, your account is dead forever. "You will need to create a new Apple ID," Apple writes, and that is guaranteed to be annoying at best.

And there are two kinds of access that two-factor authentication doesn't protect:

- It doesn't prevent e-mail from being accessed with just the knowledge of the password. Someone could still retrieve your e-mail from a me.com, mac.com, or icloud.com address with just the account name and password. That would in turn still let an attacker invoke password resets for other services that you set up using an Apple-managed address.

- You can log into the iCloud Web site with just the password, and use all the services there, including Mail, Contacts, Calendar, Notes, Reminders, Documents in the Cloud, and even Find My iPhone, from which your devices can be erased (you are backing them up, aren't you?).

Finally, if you made any significant changes to your Apple ID account in the last few days, Apple won't let you turn on two-factor authentication for three days. And if your Apple ID password is too weak for Apple's tastes (see "FlippedBITS: Four Password Myths,") Apple forces you to change it, and then forces you to wait for three days.

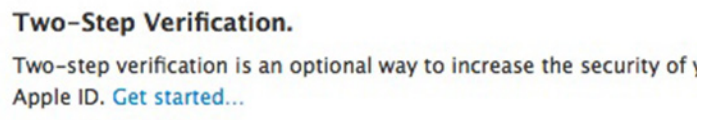
Enable Apple's Two-Factor Authentication — If you're ready to go, follow the steps listed in Apple's support note if you're in a supported country, or read our version below. (Apple has rolled out two-factor authentication in the United States, the United Kingdom, Australia, Ireland, and New Zealand, and plans to add additional countries over time. Perhaps it's a localization issue.)

1. Navigate to the My Apple ID site, click Manage Your Apple ID, and log in using your current account information.

2. Click Password and Security on the left, answer the security questions shown, and click Continue.

3. Under the "Two-Step Verification" heading and text at the top, click the Get Started link.

4.

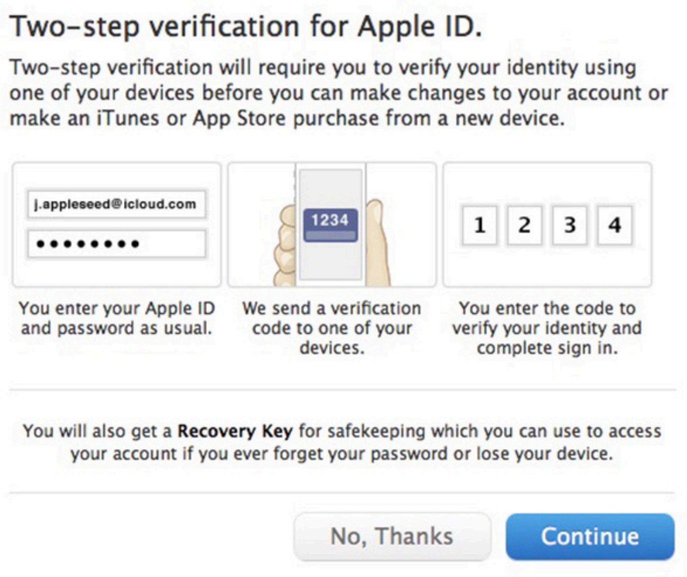


Two-Step Verification.

Two-step verification is an optional way to increase the security of
Apple ID. Get started...

5. Apple then presents three screens of information, benefits, and warnings. Read each one and click Continue on the first two, then Get Started on the last one.

6.



Two-step verification for Apple ID.

Two-step verification will require you to verify your identity using one of your devices before you can make changes to your account or make an iTunes or App Store purchase from a new device.

j.appleseed@icloud.com

••••••••

You enter your Apple ID and password as usual.

1234

We send a verification code to one of your devices.

1 2 3 4

You enter the code to verify your identity and complete sign in.

You will also get a **Recovery Key** for safekeeping which you can use to access your account if you ever forget your password or lose your device.

7. Apple displays a list of iOS devices associated with your account and lets you add SMS numbers for mobile phones. When you are finished verifying devices, click Continue.

— If you click Verify, Apple sends a code to the associated device via Find My iPhone. But, cleverly, if your device is locked with a PIN, unlike an SMS or iMessage, Apple prompts you to unlock iOS first to get the code. You may have problems if you have multiple Apple IDs because Find My iPhone can be associated with only one Apple ID. For instance, if you use foobar@icloud.com for calendars and contacts on an iPad, that's the account Find My iPhone will use, and you won't be able to associate that iPad with another Apple ID registered under foobar@example.com.

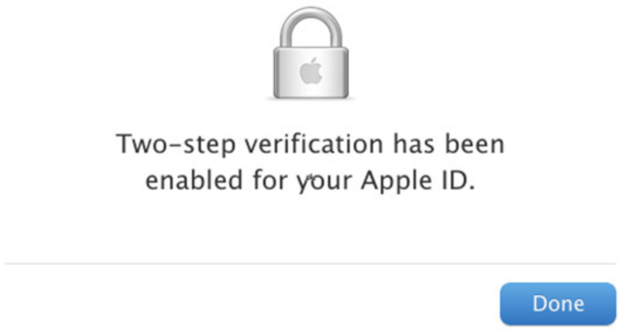
— If you click "Add an SMS-capable phone number," Apple sends the code in an SMS message. That works for connecting an iPhone that's associated with a different Apple ID via Find My iPhone or a completely different mobile phone, even one owned by someone you trust. Happily, the SMS message is free.

8. Apple now provides you with a 14-character recovery key that, if lost, cannot be recovered by anyone. Click Continue or Print Key to proceed. Apple recommends you write down your recovery key and don't store it on your Mac. That's reasonable advice, although if you have a tool that lets you store items with strong encryption (such as 1Password or Yojimbo) and secure that tool's database with a strong password that's not stored on the computer, you're not tempting fate.

9. You have to re-enter the recovery key to prove that you really wrote it down! Type it in again, and click Confirm, which lights up only if you've entered the key correctly.

10. A final warning screen explains once again how completely messed up your life will be if you lose two or three of the elements required to reset your account. Select “I Understand the Conditions Above” and click “Enable Two-Step Verification.” The Manage Your Security Settings page now shows “Two-step verification is enabled.”

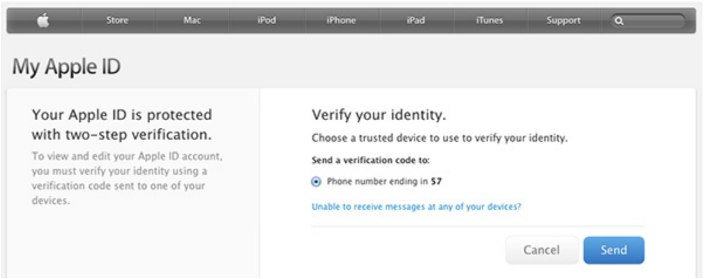
11.



Two-step verification has been enabled for your Apple ID.

You will receive e-mail notification of the change to all associated accounts immediately afterwards – and I do mean immediately, as mine arrived within a few seconds.

From then on, any time you access one of Apple’s protected services, such as the My Apple ID site’s Manage My Apple ID section, you’re asked which method you want to use to verify. Select it and proceed, and a code is sent. Enter that code, and you’re all set.



My Apple ID

Your Apple ID is protected with two-step verification.

To view and edit your Apple ID account, you must verify your identity using a verification code sent to one of your devices.

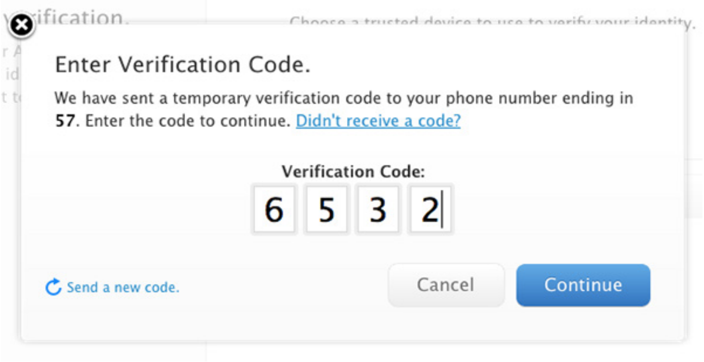
Verify your identity.

Choose a trusted device to use to verify your identity.

Send a verification code to:

● Phone number ending in 57

Unable to receive messages at any of your devices?



Enter Verification Code.

We have sent a temporary verification code to your phone number ending in 57. Enter the code to continue. Didn't receive a code?

Verification Code: 6 5 3 2

Not a Universal Solution — Two-factor authentication doesn’t solve all problems associated with validation and identity theft, but it solves some of the most important ones: password resets for account hijacking, purchases made through Apple-related services on new devices, and phone-based social engineering.

I’ve turned it on for the account I use for purchasing items, and recommend the same for all of you. Just make sure you have all your ducks and devices in a row (associated with the appropriate Apple ID and at hand) before you start!

By Joe Kissel

FlippedBITS: Four Password Myths

In the course of writing “Take Control of Your Passwords,” I came across — and attempted to debunk — quite a few myths involving password security. Of course, I encourage you to buy the book to read about password problems and my recommended solutions in detail, but for this installment of FlippedBITS, I want to focus on four extremely common misconceptions about passwords, all of which can lead to dangerous behavior.

1: Nine Is Enough -- I want to begin with a myth I propagated myself in my now-obsolete 2006 book “Take Control of Passwords in Mac OS X.” Although what I said in that book was reasonable based on the available data at the time, I grossly underestimated the rate of technological progress. So, I hereby retract and apologize for a particular piece of advice I gave back then: I said that if you chose a random 9-character password consisting of upper- and lowercase letters, digits, and punctuation, you’d be effectively safe from any attack, because it would take centuries, on average, for even a supercomputer to crack such a password by brute force.

Well, it turns out that I was off by a few orders of magnitude. Today, with off-the-shelf hardware and freely available cracking software, a nine-character password can be broken in a *maximum of five and a half hours* (that’s maximum, not minimum!). If your password contains nine or fewer characters, regardless of how random it may be, it’s about as unsafe as a Wi-Fi connection protected with WEP (which is to say, safe against only the most casual snooping).

If nine characters are too few these days, how long should a password be? I wish I could give you a straight answer, but the truth is "it depends." For example, I could claim, with some justification, that a random 14-character password is effectively safe from brute-force attacks given today's technology. But I'd have to qualify that in a few different ways.

First, I have no idea what tomorrow's technology will look like. Maybe a few years from now, someone will develop a quantum computer that can crack any 14-character password in the blink of an eye. I don't expect that to happen so soon, but I'd be foolish to bet against it.

Second, not all encryption techniques are equally secure. A password that's protected with a weak encryption algorithm might be crackable in seconds, whereas the same password, encrypted with a better method, could thwart a brute-force attack for years. Related to this is that some password security systems put additional barriers in place to slow down the rate at which passwords can be guessed. Although these aren't foolproof (as I discuss in a moment), they can, in certain situations, give a simple password much higher effective strength.

Third, length isn't the only factor that affects a password's strength. As illustrated brilliantly in the xkcd comic Password Strength, even a password consisting entirely of lowercase English words (such as correct horse battery staple) can be just as strong as a shorter but more random password with a mixed character set. That's because a password's entropy (a mathematical approximation of how hard the password is to guess) can come from length, character set complexity, randomness, or any combination of these. Higher-entropy passwords are more resistant to automated attacks, but there's more than one path to entropy. (If you'd like to test a given password's entropy, there are many online tools that let you do so. I quite like the zxcvbn tool for this purpose.)

We can take some comfort in the fact that each additional character in a password increases its strength exponentially. So, if we were to restrict ourselves to just 26 lowercase letters, a 10-character password wouldn't merely be 10 percent better than a 9-character password — it would be 26 times better! There are over 5 trillion possible passwords consisting of nine lowercase letters (26^9), but make it ten letters (26^10), and there are more than 141 trillion possibilities. That means a system that can crack a 9-character random password in 5.5 hours could take over 500 hours to crack a 10-character random password — a huge difference.

Even so, 500 hours is too little for my comfort. You could make that more than 500 years by choosing a 12-character password, which certainly seems safe enough for all practical purposes. But then, that's what I thought about 9-character passwords seven years ago. So, when I suggest 14 as a safer number, I'm building in enough of a buffer to account for a few years of technological development, not in any way saying that such a password will in fact be uncrackable for the over 4,000 millennia it would take at today's rate.

2: Old Tricks from Old Dogs -- I've encountered quite a few people — including some major names in the Mac world you'd recognize — who have developed mnemonic techniques for creating and remembering passwords that they imagine to be quite strong. Although specifics vary, there tends to be a consistent element or easily constructed pattern in each password, along with some site-specific portion. For example, maybe I use zombieGooCats for Google and zombieAppCats for Apple. (In reality, most people I know who do this sort of thing have far more sophisticated techniques, but you get the general idea.)

I myself once (cough) advocated such an approach, but I've since seen the light. The problem with all such tricks — and that also goes for "leet" or "1337" (replacing letters with similar-looking numbers), using patterns of keys on a keyboard, and so on — is that no matter how clever you think you are, hackers and their advanced cracking algorithms are smarter. These tools can test a vast number of subtle patterns that few humans would notice, which means even a fairly long, fairly random-looking password might in fact be quite easily guessable. Because remember, we're not worried so much about humans guessing your password but about machines guessing it, and machines are likely to test lower-entropy passwords — especially those based on common mnemonic techniques — long before higher-entropy passwords. (And, if you use the same technique to construct all your passwords from patterns, an attacker who learns one or more of your passwords has an even bigger leg up in guessing the rest.)

More to the point, any technique that relies on your brain for creating and remembering all your passwords is, in my opinion, a waste of mental effort that could be put toward more useful pursuits, such as thinking up bad puns. We have computers and iPads and iPhones and other devices to do this sort of tedious work for us, and they're much better at it than we are. Let a password manager such as 1Password or LastPass generate, remember, and enter passwords for you, and then you can make them as long and random as you like — it's no more effort for an app to make a 32-character password than a 10-character one. Sure, you'll still need to remember a few passwords, but if you're doing it right, it's only a few. (I have only 5 passwords memorized, out of more than 600.)

3: One Password to Rule Them All -- Speaking of password managers, these tools make it easy to create a unique random password for every single site and service that uses passwords, and I recommend doing so. I can't emphasize strongly enough what a bad idea it is to use the same password in more than one place — even if it's a great password. The fact that reusing passwords is entirely unnecessary if you rely on an automated tool makes it that much more egregious an offense.

Why is it so bad to reuse passwords? Well, it seems like every week or so, there's another news report about some big company experiencing a security breach of some sort in which thousands or even millions of passwords are lost, stolen, leaked, or hacked. This happened recently to Evernote; before that, a long list of other companies had passwords compromised – Facebook, LinkedIn, Twitter, and more. You can bet this trend will continue.

Now, if someone hacks Amazon.com's servers and gets your password, that's bad news, no question about it. But if all your passwords are unique, at least the damage will be limited to that one account. On the other hand, if you use the same password for iCloud, PayPal, Twitter, Gmail, and so forth, you run the very real risk that the attacker may try your password at all those other sites, too, doing considerably more damage.

I'm saying: using unique passwords — even strong unique passwords — doesn't guarantee security. But it does enable you to contain the damage if your password for any one site is compromised. The people most likely to be harmed by password breaches are those who are oblivious to the problem of password reuse. Don't be one of them!

4: Online vs. Offline Attacks -- Earlier, I mentioned that some sites and services put barriers in place to slow down or derail automated attacks. For example, if you mistype your password once, you might get one or several additional chances to enter it — but with increasing time delays between guesses. And if you enter it incorrectly several times in a row, you might be locked out entirely for a period of time, or until you take some independent action to confirm your identity. The whole point of these barriers is to prevent an automated system from trying many passwords per second until it breaks into your account.

While it's an excellent idea for developers to employ such barriers, they aren't as strong as they might appear. That's because most successful attacks don't go through the front door, as it were. The real danger comes when, due to a leak or security breach of some kind, someone gets hold of an encrypted file or database that holds all the passwords for a site. With the file in hand, they can perform what's known as an "offline" attack — they hammer on the raw file with automated tools that check billions of possible passwords per second. Because they've entirely circumvented the security measures that slow down guessing, they can potentially decrypt massive numbers of passwords in a short period of time. (I'm simplifying the story here. Smart developers can also use a combination of techniques — the key terms to look for are "salting" and "hashing" — to frustrate offline attacks, but all too often, a programming error or infelicitous security choice leaves gaping holes that hackers can exploit.)

So, don't assume you can use a short, simple password because you can't see any way an attacker could try billions of passwords a second. You'd be surprised what someone can do, particularly given physical access to the computer where the password is stored. Your best defense is to use high-entropy passwords (which take longer to guess) and make sure each one is unique.

Don't Worry, Be Happy If I've increased your anxiety about passwords by telling you what's wrong with techniques you depend on, I'm sorry. Well, only a little bit sorry, because I want you to have just enough discomfort that you take action to improve your password security and reduce the chance that bad things could happen to your digital life. For extensive details on passwords, including further threats and risks you might face — and my stress-free, three-point strategy for password security — please pick up a copy of "Take Control of Your Passwords."

by Adam C. Engst

OS X 10.8.3 Mountain Lion Fixes Nagging Bugs

With OS X Mountain Lion 10.8.3 Update and the included Safari 6.0.3, Apple has squashed numerous nagging bugs, many of which were extremely specific and were thus overlooked in the larger 10.8.2 release from nearly six months ago (see "OS X 10.8.2 Eases Notification Center, Messages Frustrations," 19 September 2012). The free update is available via the Mac App Store, with delta (540.46 MB – from 10.8.2) and combo (793.69 MB – from any version of 10.8) updaters now ready for download from the Apple Support Downloads site. Although we haven't noticed any problems yet, we recommend holding off on the update for at least a few days until we've seen if it introduces any new issues. Let's take a look at the details.

Ding dong, the file URL bug is dead! See "A Simple Text String that Crashes Most Mac Applications" (4 February 2013). This bug was minor, but embarrassing, so it's nice that Apple has addressed it.

The Contacts app fixes several printing-related bugs, including one that caused cards to print out of order and another that caused addresses to print in the wrong location. We still mostly print with BeLight Software's more-capable Labels & Addresses, so we've not run into these problems (see "Labels & Addresses Restores Holiday Card Sanity," 12 December 2008).

If you use Boot Camp in favor of VMware Fusion or Parallels Desktop, and you want to stay up to date with the latest developments on both sides of the fence, 10.8.3 adds support both for installing Windows 8 and for Macs with 3 TB drives.

Eye candy lovers will be pleased to learn that 10.8.3 finally brings back to Mountain Lion's Slideshow screensaver the capability to display photos from subfolders, and also fixes a bug that could cause the desktop picture to change after logging out or restarting. If you've noticed wackiness on the screen after waking from sleep, that should be a thing of the past too.

Listen up for two audio-related fixes, one that prevents an audio stuttering problem on 2011 Macs, and another that could cause Logic Pro to become unresponsive when using certain plug-ins.

On the networking side, 10.8.3 promises reliability enhancements when using a Microsoft Exchange account in Mail, claims improved compatibility with IMAP servers in the Notes app, prevents Messages from displaying messages out of order after waking from sleep, and includes fixes for two Active Directory bugs that could cause delays on high latency networks and lock out users after accessing the Security & Privacy pane of System Preferences.

Safari 6.0.3 improves performance when scrolling on Facebook and while zoomed in on a Web page, plus while viewing Web pages with plug-in content. Also included are bug fixes for an erroneous alert claiming that bookmarks can't be changed, duplicate bookmarks on iOS devices after editing them in Safari on the Mac, incorrect access to unfiltered search results when searching Google with Parental Controls enabled, and a problem that prevents Safari from restoring the correct page position when you navigate back to a previous page.

As always, both 10.8.3 and Safari 6.0.3 address numerous security vulnerabilities. Safari 6.0.3 fixes no less than 15 WebKit memory corruption bugs, plus a pair of cross-site scripting attacks. 10.8.3's security fixes span the gamut, addressing components and apps such as Apache, CoreTypes, International Components for Unicode, Identity Services, ImageIO, IOAcceleratorFamily, the kernel, Login Window, Messages, PDFKit, and QuickTime. Plus, the update no longer allows incorrect SSL certificates.

There's also mention of a malware removal tool that Apple says will run on installation and will remove most common variants of malware – you're alerted only if malware is found.

As noted at the start, although the changes in both 10.8.3 and Safari 6.0.3 are welcome, there's no telling if Apple has inadvertently introduced new problems, so unless you're being vexed daily by something that these updates fix, we recommend holding off on this update until early adopters give the all clear.

April Software Review

It has been awhile since we last printed this discussion about updating your system. It seems like a good time to dust it off and present it again...

Apple currently uses two versions of updates:

• The Update version contains the complete versions of all files/packages to be updated. It is used only for updating the immediately previous version of Mac OS X. It is a smaller download and will thus download more quickly. For example, this month Mac OS X Update 10.8.3 should be just used to update Mac OS X 10.8.2

• The Combo Update version update contains the complete versions of all files/packages to be updated, as well as all updated files/packages from all preceding updates to your version. For example, this month Mac OS X Combo Update 10.8.3 will update any version of OS X 10.8.

We recommend the following procedure when applying a System Update:

1. Consider backing up your current system with Carbon Copy Cloner or SuperDuper. OS X cannot be backed up using drag and drop — there are many important, but invisible, files that will not get backed up.

2. Make sure your hard drive is in good shape: Run Disk Utility's Repair Disk function (or use a third-party drive utility such as DiskWarrior or TechTool Pro).

3. If you have any FireWire devices connected, turn them off and disconnect them before installing the update. This includes iPods, as the iPod is a FireWire hard drive.

4. Install the update.

5. Do not interrupt the update process. The installation of incremental Mac OS X updates (or any significant system updates for that matter) should never be interrupted by putting the system to sleep, quitting the installation application, or even performing other system operations that could potentially interfere with the process.

5. After rebooting, again run Repair Disk Permissions.

6. If you have significant problems with the new updated OS, remembered the often repeated last resort advice from MacFixIt: Re-apply using the Combo version!

Using this update procedure avoids many of the common problems incurred after each update to OS X.

Apple Updates

ProApps QuickTime Codecs v1.0.2

Mar 28, 2013 - 1.14 MB

System Requirements
- OS X 10.5.6 or later
- QT 7.6 or later

This update adds the following video codecs for use by QuickTime-based applications:
- Apple Intermediate Codec
- Apple ProRes
- AVC-Intra
- DVCPRO HD
- HDV
- XDCAM HD / EX / HD422
- MPEG IMX
- Uncompressed 4:2:2
- XAVC

This update is recommended for all users of Final Cut Pro X, Motion 5, or Compressor 4.

iOS 6.1.3 Software Update

Mar 19, 2013

System Requirements
- iPhone 3GS and later
- iPad 2 and later
- iPod touch 4th generation and later
- iPhone 5

This update contains improvements and bug fixes, including:
- Fixes a bug that could allow someone to bypass the passcode and access the Phone app
- Improvements to Maps in Japan

Boot Camp Support Software 5.0.5033

Mar 14, 2013 - 553.62 MB

System Requirements
- MacBook Air (Mid 2011) or later
- MacBook Pro (Mid 2010) or later
- * MacBook Pro 13 inch-Mid 2010 is not supported
- Mac Pro (Early 2009) or later
- Mac mini (Mid 2011) or later
- iMac (Mid 2010 or later)
- Windows 7 x64, Windows 8. x64

This download contains the Windows Support Software (Windows Drivers) you will need to support Windows 7 on your Mac.

Security Update 2013-001 (Lion)

Mar 14, 2013 - 31.42 MB

System Requirements
- Mac OS X 10.7.5

Security Update 2013-001 is recommended for all users and improves the security of Mac OS X.

Security Update 2013-001 (Snow Leopard)

Mar 14, 2013 - 316.63 MB

System Requirements
- Mac OS X 10.6.8

Security Update 2013-001 is recommended for all users and improves the security of Mac OS X.

Boot Camp Support Software 4.0.4131

Mar 14, 2013 - 664.08

System Requirements
- MacBook Air (11-in, Mid 2011)
- MacBook Air (13-in, Mid 2011)
- Mac mini (Mid 2011, Intel graphics)
- Mac mini (Mid 2011, AMD graphics)
- Mac mini Server (Mid 2011)
- Windows 7

This download contains the Windows Support Software (Windows Drivers) you will need to support Windows 7 on your Mac.

Boot Camp Support Software 4.0.4255

Mar 14, 2013 - 1 GB

System Requirements
- MacBook Pro (15-in, Mid 2012)
- MacBook Pro (13-in, Mid 2012)
- Windows 7

This download contains the Windows Support Software (Windows Drivers) you will need to support Windows 7 on your Mac.

Boot Camp Support Software 4.0.4326

Mar 14, 2013 - 894.44 MB

System Requirements
- MacBook Pro (Retina, 15-in, Mid 2012)
- MacBook Air (11-in, Mid 2012)
- MacBook Air (13-in, Mid 2012)
- Windows 7

This download contains the Windows Support Software (Windows Drivers) you will need to support Windows 7 on your Mac.

Boot Camp Support Software 4.0.4033

Mar 14, 2013 - 601.76

System Requirements
- MacBook (13-in, Late 2006 & Mid 2007)
- MacBook (13-in, Late 2007)
- MacBook (13-in, Early 2008)
- MacBook (13-in, Late 2008)

- MacBook (13-in, Early 2009 & Mid 2009)
- MacBook (13-in, Late 2009)
- MacBook (13-in, Mid 2010)
- MacBook Air (13-in, Early 2008)
- MacBook Air (13-in, Late 2008 & Mid 2009)
- MacBook Air (11-in, Late 2010)
- MacBook Air (13-in, Late 2010)
- MacBook Pro (17-in, Core 2 Duo, Late 2006)
- MacBook Pro (15-in, Core 2 Duo, Late 2006)
- MacBook Pro (15-in & 17-in, Mid 2007)
- MacBook Pro (15-in & 17-in, Early 2008)
- MacBook Pro (15-in, Late 2008)
- MacBook Pro (17-in, Early 2009 & Mid 2009)
- MacBook Pro (15-in, Early 2009)
- MacBook Pro (15-in, Mid 2009)
- MacBook Pro (13-in, Mid 2009)
- MacBook Pro (17-in, Mid 2010)
- MacBook Pro (15-in, Mid 2010)
- MacBook Pro (13-in, Mid 2010)
- MacBook Pro (13-in, Early 2011 & Late 2011)
- MacBook Pro (15-in, Early 2011 & Late 2011)
- MacBook Pro (17-in, Early 2011 & Late 2011)
- Mac Pro (Mid 2006)
- Mac Pro (Early 2007)
- Mac Pro (Early 2008)
- Mac Pro (Early 2009)
- Mac Pro (Mid 2010)
- Mac mini (Mid 2007)
- Mac mini (Early 2009 & Late 2009)
- Mac mini (Mid 2010)
- iMac (20-in, Late 2006)
- iMac (24-in, Late 2006)
- iMac (20-in & 24-in, Mid 2007)
- iMac (20-in & 24-in, Early 2008)
- iMac (20-in, Early 2009 & Mid 2009)
- iMac (21.5-in & 27-in, Late 2009)
- iMac (27-in, Late 2009)
- iMac (21.5-in, Mid 2010)
- iMac (27-in, Mid 2010)
- iMac (21.5-in, Mid 2011 & Late 2011)
- iMac (27-in, Mid 2011)
- Windows 7

This download contains the Windows Support Software (Windows Drivers) you will need to support Windows 7 on your Mac.

Boot Camp Support Software 4.1.4586
Mar 14, 2013 - 414.74 MB

System Requirements
- Mac mini (Late 2012)
- Mac mini Server (Late 2012)
- MacBook Pro (Retina, 13-in, Mid 2012)
- iMac (21.5-in, Late 2012)
- iMac (27-in, Late 2012)
- Windows 7 x64

This download contains the Windows Support Software (Windows Drivers) you will need to support Windows 7 on your Mac.

OS X Mountain Lion Update v10.8.3
Mar 14, 2013 - 540.46 MB

System Requirements
- OS X Mountain Lion v10.8.2

The 10.8.3 update is recommended for all OS X Mountain Lion users and includes features and fixes that improve the stability, compatibility, and security of your Mac, including the following:
- The ability to redeem iTunes gift cards in the Mac App Store using your Mac's built-in camera
- Boot Camp support for installing Windows 8
- Boot Camp support for Macs with a 3TB hard drive
- A fix for an issue that could cause a file URL to quit apps unexpectedly
- A fix for an issue that may cause Logic Pro to become unresponsive when using certain plug-ins
- A fix for an issue that may cause audio to stutter on 2011 iMacs
- Includes Safari 6.0.3

OS X Mountain Lion Update v10.8.3 (Combo)
Mar 14, 2013 - 793.69 MB

System Requirements
- OS X Mountain Lion v10.8

The 10.8.3 update is recommended for all OS X Mountain Lion users and includes features and fixes that improve the stability, compatibility, and security of your Mac, including the following:
- The ability to redeem iTunes gift cards in the Mac App Store using your Mac's built-in camera
- Boot Camp support for installing Windows 8
- Boot Camp support for Macs with a 3TB hard drive
- A fix for an issue that could cause a file URL to quit apps unexpectedly
- A fix for an issue that may cause Logic Pro to become unresponsive when using certain plug-ins
- A fix for an issue that may cause audio to stutter on 2011 iMacs
- Includes Safari 6.0.3

MacBook Pro Retina SMC Update v1.1
Mar 14, 2013 - 504 KB

System Requirements
- OS X 10.7.5 or later
- OS X 10.8.2 or later

This update resolves a rare issue where users may experience slow frame rates when playing graphics-intensive games on the 15-inch MacBook Pro with Retina Display. It also includes bug fixes for Power Nap, wake from sleep and fan control.

Java for OS X 2013-002
Mar 4, 2013 - 63.84 MB

System Requirements
- OS X Lion v10.7 or later
- OS X Mountain Lion v10.8 or later

Java for OS X 2013-002 delivers improved security, reliability, and compatibility by updating Java SE 6 to 1.6.0_43.

On systems that have not already installed Java for OS X 2012-006, this update disables the Java SE 6 applet plug-in. To use applets on a web page, click on the region labeled “Missing plug-in” to download the latest version of the Java applet plug-in from Oracle.

Please quit any web browsers and Java applications before installing this update.

Java for Mac OS X 10.6 Update 14
Mar 4, 2013 - 69.32 MB

System Requirements

- Mac OS X v10.6.8 Snow Leopard

Java for Mac OS X 10.6 Update 14 delivers improved security, reliability, and compatibility by updating Java SE 6 to 1.6.0_43.

On systems that have not already installed Java for Mac OS X 10.6 update 9 or later, this update will configure web browsers to not automatically run Java applets. Java applets may be re-enabled by clicking the region labeled “Inactive plug-in” on a web page. If no applets have been run for an extended period of time, the Java web plug-in will deactivate.

Please quit any web browsers and Java applications before installing this update.

by Christopher Breen

Mac 911

When HandBrake won’t rip your DVDs

Reader Steven Pollock seeks a digital copy of a movie he recently purchased. He writes:

I read Macworld’s story about how to rip DVDs with HandBrake and I’m having a problem. I’d like to rip a DVD that I recently purchased so that I can view it on my iPad. But when HandBrake starts scanning it, it crashes. I’ve tried it multiple times and I’m not having any luck. Is there a trick to it?

There is. But before we get into it, run your eyes over the boilerplate text that we include with these kinds of articles:

[Editor’s note: The MPAA and most media companies argue that you can’t legally copy or convert commercial DVDs for any reason. We (and others) think that, if you own a DVD, you should be able to override its copy protection to make a backup copy or to convert its content for viewing on other devices. Currently, the law isn’t entirely clear one way or the other. So our advice is: If you don’t own it, don’t do it. If you do own it, think before you rip.]

I’ll add this little bit to the boilerplate: Many of us now own Blu-ray players and many Blu-ray discs come with digital copies of the movies contained on those discs for exactly this purpose. With a clean conscience you get the copy that you believe is yours to own. Problem is, some of these digital copies expire after awhile. If you don’t act before the expiration date to get yours, you’re out of luck and must use other means, such as ripping the DVD copy that’s often included in the Blu-ray package. And, of course, there are lots of DVDs and Blu-ray discs sold that don’t offer digital copies.

With that out of the way, onward. As you might imagine, those responsible for making and selling movies packaged on DVD and Blu-ray are not happy that some loathsome individuals enjoy their content without paying for it. (I’m looking at you, Netflix rip-it-and-keep-it-forever subscribers.) And so they devote some resources to undermining tools such as HandBrake by developing new copy protection schemes. It sounds to me like you’ve encountered one such scheme that causes HandBrake to blow up when it scans discs for their main titles.

One way around this is to tell HandBrake exactly which title you’d like it to rip rather than having it scan the entire disc (which is its default behavior) and crash in the process. But that disc contains loads of titles, so how are you supposed to learn which is the correct one?

Easy enough. Launch DVD Player (found in the Applications folder), play it, walk your way through the junk that appears before the movie, and finally play the main feature. From DVD Player’s Go menu choose Title and look for the checked title number. This title represents the main feature. (Yes, this is the same technique I described in HandBrake and the 99 Title DVD Mystery.) Keep this title number in mind and launch HandBrake,

In HandBrake choose File > Open Source (Title Specific). In the sheet that appears, navigate to the DVD, select its VIDEO_TS folder, and click Open. In the sheet that replaces it, enter the title number in the appropriate field. (Where it says Scan Title Number X for nameofmovie.) Click the Open Title button and HandBrake will select that title. Now choose the preset you wish to use (Apple TV 2, for example), and click HandBrake’s Start button. HandBrake will set about ripping the disc’s correct title (without crashing).

Making Dropbox your default folder

Reader Gil Cranston would like to save a step or two when saving files. He writes:

I'm a pretty happy Dropbox user who spends a lot of time on the road. But I sometimes forget to put the files I'm working on at the office in my Dropbox folder. Any hints on ways to ensure this doesn't happen?

I can offer a couple, yes. The first is dead simple but it will cost you $35. That $35 solution is St. Clair Software's Default Folder X. This much-beloved-by-Macworld's-Dan-Frakes utility allows you to choose a… well, default folder for saving documents within any application.

For example, if the Excel documents you work on are created with your job in mind, you can configure Default Folder so that these documents are saved to your Dropbox folder (or, better yet, a folder within it) by default. What makes this better yet is that Default Folder can create a separate default destination for each application you use (see the image above). So, use an Excel Docs folder within your Dropbox folder for your spreadsheets, Word Docs for those files, and a PDFs Folder for… well, you know.

Another benefit of Default Folder is that it can work around Mountain Lion's desire to save certain kinds of documents to iCloud (those documents spawned from the iWork applications, TextEdit, and Preview). In the past, Default Folder couldn't defeat the Documents in the Cloud feature that made iCloud the default destination for saving documents within these applications. It now can.

Or you can save the $35 by slightly rejiggering the Finder and changing your work habits. While I still greatly prefer the Default Folder solution, you can instead locate your Dropbox folder (placed within your user folder by default) and drag it into the top position in a Finder window's sidebar. Now, when you save a file within any application, click on the Where pop-up menu in a Save dialog box and you'll find that your Dropbox folder is at the top of the list.

How to synchronize e-mail signatures

Reader Ned Chessman is curious about a Mail feature. He writes:

I have a recent iMac and I'm planning to purchase a MacBook Air. I've created a lot of signatures in Mail on my iMac and I'd hate to have to recreate them on my laptop. Is there any easy way to transfer those signatures to the laptop's copy of Mail?

If you have the same iCloud account set up on each computer and you've configured each to synchronize e-mail (you do this in the iCloud system preference) you'll find that your signatures will magically appear on the MacBook shortly after you launch Mail.

However, you may find that they're not attached to a particular account. Instead, when you open Mail's preferences and click on Signatures you find your complete collection of signatures when you select the All Signatures entry at the top of the account list, but no signatures attached to specific accounts. Should you wish for them to be so attached you must drag them to the correct account.

If that seems like a terrible bother because you have dozens and dozens of signatures attached to multiple accounts, you can copy the Signatures folder from your iMac to the MacBook. The location of that folder is youruserfolder/Library/Mail/V2/MailData. (To navigate to the Library folder within your user folder, hold down the Option key in the Finder and choose Go > Library.)

Just place the Signatures folder in the same location on the MacBook (replacing the original Signatures folder) and then launch Mail. Provided that you have the same accounts set up on the MacBook as you do on the iMac, your signatures should be attached to their correct accounts.

[Macworld Senior Editor Christopher Breen is the author of "Secrets of the iPod and iTunes (6th edition)," and "The iPod and iTunes Pocket Guide (4th edition)" both from Peachpit Press and
"OS X 10.5 Leopard Essential Training (video)" from lynda.com Find Chris' books at www.amazon.com and www.peachpit.com. Get special user group pricing on Macworld Magazine! Subscribe today at http:// www.macworld.com/useroffer

Share Keystone MacCentral with other MACaholics

Name ____

Address ____

City ______________________________ State ___ Zip __________

Home Phone ____________________ Day Phone ____________________

E-mail Address ____________________________________

Date ______________ Is this ○ Renewal or ○ New?

How did you hear about us? ____________________________

Dues for one person are ○ $20/yr. Family or Corporate dues are ○ $30/yr.

To join Keystone MacCentral, mail this form with your membership dues (payable to Keystone MacCentral) to:

Keystone MacCentral
Membership Chair
310 Somerset Drive
Shiresmanstown, PA 17011

Keystone MacCentral meetings are **usually** held at 6:30 p.m. on the 3rd Tuesday of the month at Giant Foods, Trindle & 32nd, Camp Hill