The PULP

HUGE this month:

General Meeting: Feb. 18th

Android Tablet

See you there!

New Location !!!!!

Knights of Columbus
2533 Main Street,
Glastonbury, CT

Q&A Session: 7:00PM–7:30PM
Meeting starts at: 7:30PM

Contents:

The Quiz	3
FlippedBITS: Four Password Myths	4
Five Ways to Reset a Lost Administrator Password	6
Free Internet Faxing Services: No Fax Machine Required!	8
Calendar	10

The **PULP** is published monthly by and for members of the Hartford User Group Exchange, Inc. (**HUGE**). **HUGE** is a nonprofit organization whose aim is to provide an exchange of information between users of personal computers. The **PULP** is not in any way affiliated with any computer manufacturer or software company. Original, uncopyrighted articles appearing in the **PULP** may be reproduced without prior permission by other nonprofit groups. Please give credit to the author and the **PULP**, and send a copy to **HUGE**. The opinions and views herein are those of the authors and not necessarily those of **HUGE**. Damages caused by use or abuse of information appearing in the **PULP** are the sole responsibility of the user of the information. We reserve the right to edit or reject any articles submitted for publication in the **PULP**. Trademarks used in this publication belong to the respective owners of those trademarks.

MEETING LOCATION
Knights of Columbus
2533 Main Street
Glastonbury, CT

Editor's Corner

This month the topic is a demo of an Android tablet. Upcoming in future meetings: some maintenance tips (including what a failing hard drive sounds like), Maverick pt. 2, and Father's Day gifts for geeks.

In the news: Some hackers may be in for a big payday, Google has put up $2.7 million in prizes in a Chrome hacking contest. Pwn2Own has $675 K in prize money to award.

Telefonica has a project called BeWifi that will enable internet users to borrow unused bandwidth from a nearby Wi-Fi network. Of course you and your neighbor need to be using Telefonica equipment (routers), agree to the process and live in Spain.

Apple has patented a solar-powered MacBook.

Researchers at Virginia Tech are working on a biobattery that runs on a sugar solution that has an energy-storage density 10 times that of lithium-ion batteries. Actually it is more of a fuel cell.

Other researchers have discovered a three-dimensional topological Dirac semi-metal (3DTDS) with a electronic structure similar to graphene that can exist in three dimensions and might lead to faster transistors and more compact, higher capacity hard drives.

Target, Michaels, **Neiman Marcus** and about 6 other retailers had their Point of Sale (the equipment that swipes your card) hacked. The credit & debit card information for 110+ million customers were compromised. Target may have compounded the problem by sending out an email that resembled a 'phishing' letter. Some experts think the thieves may have over-reached. Watch this space.

On the **really** good news front: A manufacturer of 3D printers has been working with Hershey to produce home 'Kisses'. If available, it will be on (top of) the gift list next year.

Stuart Rabinowitz
Editor

Here is the appropriate copyright citation and a link to the full text. articles from "Tidbits"

http://creativecommons.org/licenses/by-nc-nd/3.0/

A Little Computer Quiz

by Stuart Rabinowitz

The trivia and minutiae of the computer related world. The answers will appear next month or you can submit an answer sheet at the General Meeting. Good Luck.

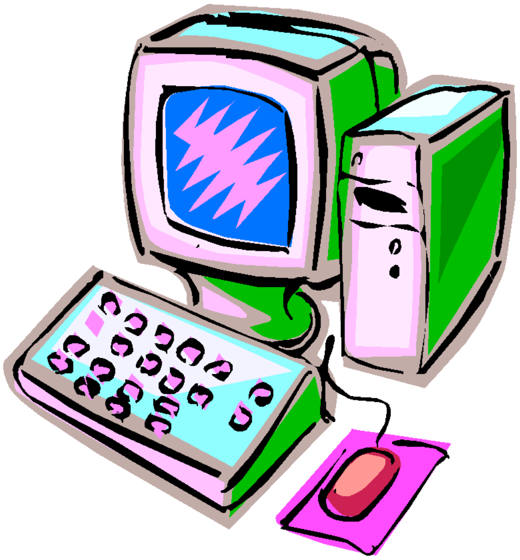
1 It's been 30 years since Apple introduced the Mac, but there was another computer company that began selling computers in 1984. What was that company?

2 Ten years earlier in 1974 a new game (still being played today) was published. What is that game?

3 Who developed the game?

4 Who was the publisher?

5 Like many people in 1984, I participated in an Apple program tied to the release of the Mac. What was the program called?



Answers to Jan., 2014 Quiz

1 What was the first cellular phone to include telephone and PDA features in one device (aka -- a smartphone)?
A The **IBM Simon Personal Communicator** was a handheld, touchscreen cellular phone and PDA

2 When was it released?
A IBM began selling it in August, 1994 and sold 50,000

3 Who was the only cellular carrier?
A BellSouth Cellular carried the phone in 15 states

4 How much did it cost?
A $1,099 without a contract

5 What was the first cell phone to be called a "Smartphone"?
A The Ericsson GS 88 "Penelope" was the first to be described as a "Smartphone", but it was not released.

FlippedBITS: Four Password Myths
----

by Joe Kissell: <joe@tidbits.com>, @joekissell
article link: <http://tidbits.com/e/13651>
13 comments

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.

<http://www.takecontrolbooks.com/passwords?pt=TB1166>

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).

<http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/>

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.)

<http://xkcd.com/936/>
<http://dl.dropbox.com/u/209/zxcvbn/test/index.html>

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.)

<http://1password.com/>
<http://lastpass.com/>

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.

cont. pg.9

Five Ways to Reset a Lost Administrator Password

by Alicia Katz Pollock: <alicia@royalwise.com>
article link: <http://tidbits.com/e/14437>

Several years ago, I was helping a client upgrade her Mac running Mac OS X 10.5 Leopard, but she couldn't remember her administrator password. Because she also couldn't find the original system CDs that shipped with her iMac, I had to resort to some advanced techniques few home users would ever be able to figure out.

Starting with 10.7 Lion, you could still call on all those options, but Apple added a method so easy that even an inexperienced user can do it — the Apple ID-based password reset. Let's explore all the options to reset a password. Which you should use depends on the specific version of Mac OS X, and how the Mac is set up.

But first, there's an important caveat about any of these methods, related to the login keychain.

Reset Login Keychain Password -- No matter which of these methods you use to reset a forgotten administrator password, it won't update the password protecting the account's login keychain, which stores all of the user's passwords. Since the keychain is protected by the now-forgotten administrator password, there's no way to get back into it. Newer versions of Mac OS X may prompt about this problem at startup; otherwise you'll need to delete the keychain and start it over again, using these steps:

1. Open Keychain Access from /Applications/Utilities, and choose Keychain Access > Preferences (Command-,).

2. In newer versions of Mac OS X, you'll see a button labeled Reset My Default Keychain in the General pane. If you have that button, click it to remove the old keychain and create a new one with the new password.

3. If that button is not present, choose Edit > Keychain List (Command-Option-L), select the login keychain, and click the minus button to delete it.

<http://tidbits.com/resources/2014-01/Delete-keychain.png>

4. Quit Keychain Access and restart the Mac. A new login keychain will start collecting and storing the passwords for Wi-Fi networks, email accounts, Web sites, and other logins as they occur.

If you can't work with Keychain Access because of something like Messages Agent constantly asking for the forgotten login keychain password, you'll have to resort to the command line, with these steps:

1. Reboot into Single User mode by restarting the Mac and holding Command-S while the system comes back up. Numerous lines of status messages will scroll by.

2. Once you have a command-line prompt, enter this command to mount the root Mac OS X drive as writable, so you can make changes to the filesystem:

```
mount -uw /
```

3. Figure out the shortname of the account you want to reset by looking through the list that results from typing this command:

```
ls /Users
```

4. Now enter this command to delete that account's login keychain, replacing shortname appropriately:

```
rm
/Users/shortname/Library/Keychains/login.keychain
```

5. Restart the Mac by typing:

```
reboot
```

When the Mac comes back up, Mac OS X should create a new login keychain.

Now let's move on to resetting the password!

1: Use the Command Line -- In early versions of Mac OS X, the command line was the best way to reset a forgotten administrator password. Even now, command-line password reset remains available, making it the most universal approach that will work in any situation. If you're not turned off by typing highly specific commands, follow these steps:

from pg. 2

1. Make a note of the user account shortname by opening the Home folder (in the Finder, choose Go > Home) and checking the folder name at the top of the window. If you can't get into the account at all, you can determine the shortname later on.

<http://tidbits.com/resources/2014-01/Home-folder-name.png>

2. Reboot into Single User mode by restarting the Mac and holding Command-S while the system comes back up. A lot of arcane status messages scroll by, and leave you with a command-line prompt.

3. Mount the root Mac OS X drive as writable, so you can make changes to the filesystem, with this command:

```
mount -uw /
```

4. For those running 10.7 Lion, 10.8 Mountain Lion, or 10.9 Mavericks, enter this command at the prompt to load Open Directory (which manages user accounts) manually, since it was deprecated in Lion:

```
launchctl load /System/Library/LaunchDaemons/com.apple.opendirectoryd.plist
```

Skip this step if you're running 10.6 Snow Leopard or earlier.

5. If you don't know the shortname of the account you want to reset, look through the list that results from typing this command:

```
ls /Users
```

6. Next, enter the following command, replacing "shortname" with the desired account's shortname:

```
dscl . -passwd /Users/shortname
```

If you get this error message, you may ignore it:

```
launchctl: Couldn't stat("/System/Library/LaunchDaemons/com.apple.DirectoryServicesLocal.plist"): No such file or directory nothing found to load
```

7. Type in the new password.

8. Restart the Mac by typing:

```
reboot
```

2: Use One Account to Reset Another -- Since 10.4 Tiger, if a Mac had multiple administrator accounts, you could log into one account to reset the password in another. This remains possible, and is one of the reasons that many people who are responsible for the Macs of less-experienced users will often create a separate administrator-level account for troubleshooting. Here are the steps you need to follow to use this approach, assuming you have the necessary access:

1. While logged in an administrator account in which you know the password, open the Users & Groups pane of System Preferences (it was called Accounts before 10.7 Lion).

2. Select the name of the user whose password you want to change, and click the Reset Password button. (You may need to click the lock icon in the lower left of the window and enter an administrator password to be able to make changes.)

<http://tidbits.com/resources/2014-01/Reset-password.png>

3. Enter the new password, the same password again for verification, and a hint in case it's forgotten again.

<http://tidbits.com/resources/2014-01/New-password-hint.png>

3: Use the Installer CD or DVD -- Up through 10.6 Snow Leopard, if the Mac had only the original administrator account, and resetting the password via the command line was too scary, you could use the original Mac OS X Install disc instead. (Actual snow leopards may be endangered, but installer discs went extinct with 10.7 Lion, so this method is only for older Macs.) Here's how:

1. With the Mac turned off, power it up, insert the disc immediately, and hold down the C key to make the Mac boot from the disc's version of Mac OS X.

2. From the Utilities menu at the top of the screen (or the Installer menu in 10.3 Panther), choose Reset Password.

3. Select the hard disk volume, and the name of the original administrator account. (Stay away from the Root account.)

4. Enter the new password, and then click Save.

5. Quit the Mac OS X Installer, and restart the Mac normally.

Apple provides a support document with more details, along with instructions for Mac OS X 10.1 through 10.3, should you run into such an ancient setup.

<http://support.apple.com/kb/ht1274>

4: Use the Recovery Partition -- Starting with 10.7 Lion, which was sold only through the Mac App Store, the installer disc was replaced by the Recovery partition, a small chunk of the boot disk that contains a stripped-down version of Mac OS X and essential utilities. To reset the administrator password when running Lion or later:

1. Restart the Mac while holding down the Option key, and double-click the icon for the Recovery partition. A Mac OS X Utilities screen appears.

2. Choose Utilities > Terminal.

3. In Terminal, type resetpassword. Rather unusually for a task performed from the command line, a graphical Reset Password window appears.

4. Select the startup volume at the top of the window, and then choose a user account from the pop-up menu. In the fields below, enter the new password, confirm it, and add an appropriate hint.

5. Click Save, and then choose Restart from the Apple menu.

5: Use Your Apple ID -- Starting with 10.7 Lion, it

cont on pg. 9

Free Internet Faxing Services: No Fax Machine Required!
by Bob Rankin, Ask Bob Rankin
www.askbobrankin.com

Reprinted with permission
http://goo.gl/Jhh9XE

Dump your fax machine, the Internet has made this dinosaur obsolete. Think of the savings on toner, paper, and time when all you really need these days is a cell phone, PDA, or PC. I have a big list of sites for you that offer free Internet faxing services. Some of them are completely free, while others offer free or limited trials. Pick the online fax service that suits you best...

FaxZero lets you send free faxes from a simple web-based interface. Just enter the sender and recipient info, type in your message, and hit the "Send Free Fax Now" button. The rich-text editor lets you add basic formatting, highlighting and fonts to your text. You can also fax a file from your hard drive. Supported file formats include PDF, Microsoft Word (DOC, DOCX or RTF), Excel spreadsheet (XLS or XLSX), image files (PNG or JPG), TXT, HTML, and PowerPoint (PPT). You can attach multiple files, but the combined size of all attachments must be 20MB or less.

And yes, it's really free to send a fax to anywhere in the USA or Canada. You can send five free faxes per day, each with a maximum of three pages. No ads are inserted on your faxed pages, but the FaxZero logo will appear on the cover page of your outgoing fax. You can even use FaxZero to fax your U.S. congressperson or senator. I've written more about FaxZero in my Send a Free Fax article.

GotFreeFax is basically a clone of FaxZero, with some minor differences. You can send 2 free faxes daily to the USA or Canada, with a 3 page per fax maximum. No ads or branding appear on the cover page. GotFreeFax supports PDF, Microsoft Word, OpenDocument Text (.odt), and Rich Text (.rtf) file formats only. One unique feature is the ability to substitute tokens in the message, such as {RECEIVER_NAME}, {RECEIVER_COMPANY}, and {RECEIVER_FAX}.

PamFax is another free faxing service that offers 3 free outgoing pages (after signup) with no ads. You can also get a free fax number for inbound faxes. PamFax has an address book for convenience, integrates with Outlook, and works with popular cloud services such as DropBox, Google Drive, and SkyDrive.

PopFax is yet another free fax sending service. Like the others, you can input a brief text message, or upload a document from your hard drive. But I can't recommend PopFax for several reasons. In the Terms of Use on their website, it says that PopFax does not guarantee "the possible alteration of the data sent by the User nor the service availability." It also says they are not liable for damage "following to an alteration of the User data transfer." This could be badly translated legal mumbo-jumbo, but yikes! Also my Chrome browser crashed when trying to send a DOC file with PopFax. On another attempt, it said my fax number was "invalid." After sending a test fax to another number, it never arrived. Of course, your mileage may vary, but with so many other choices, I'd steer clear of PopFax.

Sign up with K7, a messaging system that will send free faxes and voicemail to your email address, with an option to view or listen to your messages via the web. You get a free fax/voicemail number which you can give to your family, friends, and business buds. Just sit back and wait for the faxes to start dropping into your inbox as email attachments. If a K7 number is inactive for 30 days (no incoming voice or fax messages), it will be terminated. K7 cannot be used to send outgoing faxes. My companion article Free Inbound Faxing goes into more detail about Faxaway, an almost-free service that forwards incoming faxes to your email.

eFax claims that they are the largest online network on the planet with over a million subscribers in 2,500 cities and 27 countries. Also known as Zipfax, you can send and receive faxes as email attachments. You simply use the recipient's fax number and eFax's address. The 30-day freebie allows you to send or receive up to 150 pages. If you don't cancel during the initial month, you will be charged $16.95 per month. See also Free Inbound Faxing for more details on eFax Limited Accounts, a free service that forwards incoming faxes to your email.

Nextiva Fax offers a 30-day free trial, including 500 free faxes. Send a fax by email, or send and receive faxes from Microsoft applications. Instead of hitting the print button, simply select "fax" right from Word, Excel, etc. Nextiva also lets you send and receive faxes from mobile devices. After the trial period, you'll be $8.95 per month, unless you cancel.

RingCentral is designed for small businesses, not only can you receive and send faxes via email, they can supply you with toll-free fax numbers, custom greetings, an auto-receptionist, voicemail, and multiple extensions. The company offers a 7-day free trial, during which you get 500 free fax pages. After the trial period, you'll be $7.99 per month, unless you cancel.

I couldn't find a smarphone app that sends free faxes. There's an app called scanR that's supposed to do that, but apparently it's defunct. CamScanner is a free app that turns your iPhone or Android smartphone into a scanner, fax machine and PDF creator. Take a picture of a document, receipt, business card, etc. CamScanner turns it into a searchable PDF that you can fax, print or upload to various cloud storage services. Faxing costs 99 cents per page.

from pg. 5

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."

<http://www.takecontrolbooks.com/passwords?pt=TB1166>

----
read/post comments:
<http://tidbits.com/e/13651#comments>
tweet this article: <http://tidbits.com/t/13651>

from pg 7

also became possible to use your Apple ID to reset your administrator password. It's turned on by default in the Network pane of System Preferences, but double-check to make sure.

<http://tidbits.com/resources/2014-01/Users-Groups-Apple-ID.jpg>

When this feature is active, if you enter the administrator password incorrectly at the login window three times, a popover appears with the password hint and a message saying "If you forgot your password, you can reset it using your Apple ID." Here's how to do that:

1. Click the arrow icon to open the Reset Password dialog.

2. Enter your Apple ID and its password, then click Reset Password to proceed.

3. Enter a new administrator password, verify it, and fill in the Hint field so that you'll get a memory trigger the next time you forget.
4. Click Reset Password, and you're done.

If you've also forgotten your Apple ID password, you can reset that at Apple's My Apple ID page. Doing so relies on having access to the email address associated with your Apple ID; if that email account could be compromised, allowing the administrator password to be reset by the Apple ID might provide a way that the physical security of your Mac could be attacked. If you're really worried, turn the feature off in the Users & Groups preference pane.

<http://iforgot.apple.com/>

One quirk. If you upgraded from 10.6 Snow Leopard to 10.7 Lion, you may not get the reset message after three incorrect attempts. To fix this problem while you can still access the account, open the Users & Groups preference pane, delete the affected Apple ID, and then add the same Apple ID back.

It's also important to know that encrypting your Mac's boot disk with FileVault 2 prevents you from using your Apple ID to reset your password (since the password is used in FileVault's encryption). Read this Apple support document for more information about FileVault.

<http://support.apple.com/kb/HT4790>

No Excuse for a Lost Password -- Regardless of how or why an administrator password has been lost or forgotten, there are a variety of techniques that you can use to reset it and regain full access to a Mac. These techniques aren't to be used willy-nilly, since the login keychain will be lost in the process, but whether the simple method of using an Apple ID is sufficient or you need to drop down to the command line, you should be able to get the access you need.

----
read/post comments:
<http://tidbits.com/e/14437#comments>
tweet this article: <http://tidbits.com/t/14437>

PULP Staff	
Editor	Stuart Rabinowitz
Distribution	George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and include a one-year subscription to The Pulp as well as access to the HUGE Public Domain disk libraries. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

President:	George Carbonell	860.568–0492	george.carbonell@comcast.net
Vice President	Stuart Rabinowitz	860.633–9038	s.e.rabinowitz@att.net
Secretary:	Ted Bade	860.643–0430	tbade@cox.net
Treasurer:	Charles Gagliardi	860.233–6054	epencil@att.net
Director at Large:	Richard Sztaba		richer1@aol.com
Web Manager:	Bob Bonato		wmaster@huge.org

Membership:	Richard Sztaba		richer1@aol.com
Integrated SIG:	Stuart Rabinowitz	860.633–9038	s.e.rabinowitz@att.net

February 2014

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
						1 1972 HP-35 introduced
2	3	4 2000 The Sims launched	5	6	7	8
9	10	11	12 Darwin Day & Awards	13	14 1946 ENIAC turned on	15
16	17	18 General Meeting 7 PM	19	20	21	22
23	24	25	26	27	28	