Macaholics UNANIMOUS

The Official Newsletter of the Upper Keys Macintosh Users Group — Apple User Group — September 2014 Volume 22 Issue 10

The Apple Security Model by Allan Miller

by Sue Beal

We got geeky with Apple security in August, with the help of Minions, bananas, a ten-year-old, and of course, Allan Miller!

Allan started with definition of some of the terms used throughout the evening:

BIT - one binary piece of information, which can be on or off. If you combine bits, every bit you have doubles the value that can be represented. Four bits is 2^4 ... 2 x 2 x 2 x 2, or 16.

ENCRYPTION - Allan defined it as "gobbledy gook" i.e., nonsense. You can't read it or make sense of it. You need a key or something to decrypt it.

STRONG ENCRYPTION - *practically* unbreakable encryption. It's rated in terms of how long it would take to crack.

HASH FUNCTION ENCRYPTION - Like a signature, a unique hash function can't be decrypted. It's a one-way key. Passwords are often hashed when they are stored, so that no one can come along and steal them.

SYMMETRIC ENCRYPTION - A lock with a one key.

ASYMMETRIC ENCRYPTION - A lock with two keys. One locks, one unlocks.

CERTIFICATE - Like a driver's license, this is issued by an authority to uniquely identify you.

About UKMUG

UKMUG meets at the Key Largo Library Community Room on the second Thursday of each month. Speakers begin at 7pm, and may go as late as 9pm.

Beginners can come at 6:30 with questions, and we encourage others to come and help.

Voluntary annual dues are collected in Jan-Feb-Mar: $25.

Father and son duo Allan and Theo Miller presented the Apple Security Model in August, with a little help from the Minions from Despicable Me, and a Hackintosh computer... built by Theo! Theo is 10 years old. You know how we joke about getting a 10-year-old to help us understand something technical? *Theo is the one you want!*

TRUSTED SECURITY - This is a concept. We trust certain entities. We trust a locksmith to use their knowledge for good, not theft.

TRUST NO ONE - No one else can unlock it!

Allan went on to tell a story...

continued on page two

OUR NEXT MEETING:

Thursday, Sept. 11, 2014

7pm at Key Largo Library
Community Room
MM 101.4 Oceanside

Pixelmator with Joe Kukella

Pixelmator: Image Editing for the Rest of Us! Pixelmator is a full-featured and powerful image editing application for the Mac. It gives you speedy, powerful tools that let you touch up and enhance images, draw or paint, apply dazzling effects, or create advanced composition.

While he is in the Upper Keys, Joe will be booking appointments for personal training. If you're interested in having him stop by your home or business for an hour or so to cover any Mac OS, iOS, or Adobe product (Creative Suite, Photoshop, Illustrator, InDesign) questions you have, drop him a note at joe@kukella.com.

A Mac user since 1988, Joe's work as a designer and educator gives him a unique perspective on technology, how people use it, and how to explain it. He's an Assistant Program Director for the Art Institute of Pittsburgh Online, and he hosts workshops and training focused on Macs, iPhones, and iPads for individuals and small groups. He spent five years with Macintosh Systems Solutions serving as the Service and Education Coordinator.

Beginners: Come at 6:30 for Beginner's Circle - bring your questions and get help.

Apple Security Model

continued from page one

He told the history of the "Banana Computer Company." Just for the heck of it, I'm going to call it Apple in the write-up!

In 2001, the iPod was invented, and there was a need to allow users to share their music between the desktop computer and the iPod. The was the beginnings of the iOS operating system. We synced it with a cable, at first.

Pretty soon, we needed to sync without physically plugging in, and there was this handy thing called the Internet to help. Between networking and cloud storage, we had a need to a way to protect our stuff from others.

So, how secure is the cloud? Pretty secure, says Allan, because it's encrypted. The encryption is both in the device and in the cloud, and we need one key to unlock it on all of our devices. That's where iCloud Keychain comes in.

When you hook up to the cloud and supply your Keychain encryption key, it unlocks and manages access to all your devices. It uses a **secure token**, in a "trust no one" type of security. You get 10 attempts to get in, and then you're locked out forever - even Apple can't get you access again!

Apple enforces their security over your iCal, Contacts, Backups, Photos, and Reminders with unbreakable 128-bit encryption. (That's 2^{128}!!) And iCloud uses 256 bit **symmetric encryption** on its Keychain files. Be aware - Apple does not encrypt your email. Their system administrators can read your emails.

Apple also uses **asymmetric key encryption** to send private transmissions that only the intended recipient can read. It takes an interchange: Dave (he's a Minion) asks Stuart for Stuart's locking key. Stuart gives it to him. Dave locks the transmission with Stuart's key and sends it. Stuart receives it and unlocks it with his unlocking key. Think of it like a safe deposit box, with two keys.

This is very secure but becomes unmanageable with many Minions involved. A central place for keeping track of all the keys is needed, and Keychain comes to the rescue.

Allen gets "down and geeky" with a fun presentation on security! How did he make it fun? He sandwiched all that info between Minions and bananas!

Our locking key is public in Keychain, where anyone requesting it can get it. Our private (unlocking) key remains private. Each of our devices remains uniquely encrypted.

What if you go outside of Apple?

Some things are not as secure. For example, have you ever noticed that some-

continued on page three

Graham & Joanne Thomas. Thanks, Graham, for sharing so many good articles with us!

Theo helps Jeffrey Shamon, while in the back, Allan helps Claude Bullock.

Allan & Carol Ackenhouse show Jeanne Kavanaugh something in the newsletter.

Apple Security Model

continued from page two

times text messages are blue and sometimes they're green? If they are contained in Apple's jurisdiction, they are secure and they are shown in blue. If anything causes them to not be secure, Apple alerts you by coloring them green. FaceTime works similarly.

Password Managers

Allan was asked if he recommended any particular Password Manager like 1Password or LastPass. He said they're good for online passwords. Personally, he uses TrueCrypt, an **asymmetric encryption** service. He has the only key to the vault, which is in the cloud, and inside are all of his passwords, which he can access from all of this devices.

The Future

Steve Jobs didn't like remembering passwords, so Apple came up with the thumbprint ID on the newest iPhones. Touch ID is just the beginning, says Allan.

There are bio-devices in the works that will store personal biometrics about you, to be used for identification. This is loaded in the first time you use the device. Of course, that information must also be encrypted and protected. Apple does this with a chunk of memory they call a **secure enclave** - an encrypted area. You still need a passcode to get into it to set up the fingerprint ID.

Another new technology is iBeacon, which allows devices to talk to each other without using the internet. Using Bluetooth, a product on a shelf with iBeacon can send a signal to your iPhone which tells the iPhone user about itself. It's a bounce signal. The app you use for this controls how secure it is.

There's also near-field communication, or NFC. Although useful in many application, it's also known for aiding in identity theft. There are devices that can use this technology to read the information from cards you carry in your wallet with magnetic strips... as you pass by. Many of these cards, and your Passport, carry unencrypted information about you and your accounts. The remedy is something called a Faraday cage, which creates a field of interference. Quick fix: line your wallet and Passport cover with aluminum foil!

We thank Allan and Theo for a very enjoyable evening and look forward to seeing them again.

Minions, assemble! Karen carried out the theme with decorations and refreshments.

Allan shows some of the bananas. On the left is the Hackintosh Theo made, which was used to run the presentation.

Balloon bananas were everywhere, courtesy of Kathy Miller!

Jeffrey Shamon, Mary Anne Roper, Pete Bacheler and Joanie Stark.

Theo and the Hackintosh

Allan and Theo brought an older laptop —not an Apple — running Mavericks on PC hardware! Theo told us that he started this project when he was six years old, working with Windows XP. He made Windows look like the Mac OS. Continuing his quest four years later, he used online resources he found at www.MacBreaker.com as a starting point. He was able to get his Dad's old laptop to run Mavericks. He customized his icons, as he likes the "flat style" look.

Theo also cited www.MultiBeast.com as the Hackintosher's best friend. There are a number of hardware requirements to be solved when choosing what computer to use for this, and even though he pulled it off with his Dad's laptop, Theo recommends a desktop model to start with, it's easier.

The only downside to Theo's Hackintosh is that it doesn't access the internet on WiFi, he needs an Ethernet cable.

Should we mention he was able to build his "Mac through the back door" for about $400? Should we also mention that this is technically against Apple's Terms of Service? It's still pretty damn impressive! Read more: www.hackintosh.com

Hackintosh

Think *really* different

Reducing the shakes in a movie

from J. D. Biersdorfer of The NY Times
submitted by Graham Thomas

If you have a computer with a DVD drive, enough hard-drive space and some video-editing software, you might be able to smooth out the original 8 mm camera-work enough so you can watch it without motion-sickness pills. You first need to convert digitized movies on the DVD to video files you can edit on the computer.

So-called DVD converter programs for Windows and Mac OS X are available in shareware archives, but the cross-platform HandBrake video transcoder can usually convert discs without copy restrictions to MP4 files or other video formats. Once you have converted the movies and have them on your hard drive, video stabilization software may hopefully reduce some of the original camera shake.

Free or relatively inexpensive video-editing programs for home users — like Windows Movie Maker for Windows 8, Apple's iMovie and Adobe Premiere Elements — now include video stabilization tools you can use on the clips once you import them into the program. The $20 Muvee Turbo Video Stabilizer, or plug-in software like the $100 NewBlue Stabilizer (which works with many popular video-editing programs) are among the other options. YouTube even has video stabilization tools for uploaded clips.

The software may not smooth out all the shakes, but it could make the movies easier to watch. MU

Old Pages Documents Convert with Preview!

from Harold Pinder

Harold found he had many old documents he had made in Pages, all text, that would not open after he upgraded his Mac. He googled around and found a fix, courtesy of nicolascpa in the Apple Support community:

You won't be able to edit the old Pages document but if you right click on the document in Finder you can select Open With and then select Preview. (You can also drag and drop the document onto the Pages icon in the Dock.) This will open the document in the Preview app.

You can select the entire content of the document by going to the Edit drop down menu and selecting "Select All." (Or, you can use Command A while your cursor is in the body of the document.) Copy the contents and then paste it into a document in the latest Pages.

The pasted contents will retain the same formatting as in your original document. Save this Pages document and then you can start going forward. MU

My Blackberry is not Working

There are some laugh-out-loud moments in this cute BBC sketch. http://www.flixxy.com/my-blackberry-is-not-working.htm

Sent in by Carol Ackenhausen

WHY WE STILL NEED NEWSPAPERS

I was visiting my daughter last night when I asked if I could borrow a newspaper.

"This is the 21st century," she said.

"We don't waste money on newspapers. Here, use my iPad"

I can tell you this. That fly never knew what hit him.

joe@kukella.com
305.849.1187

training, repairs, and technical support for Mac OS, iPhone & iPad, and Adobe applications for individuals, businesses, and small groups from key largo to key west. cool.

Adobe

ALL KEYS COMPUTERGUYS
YOUR MAC AND PC GURU'S

JACK BUCCELLATO

- MOBILE COMPUTING SERVICES WE COME TO YOU!
- SERVICE, SUPPORT AND EDUCATION SPECIALISTS
- MULTIMEDIA INTEGRATION (APPLETV, MUSIC, MOVIES AND PHOTOS)

305.707.7165
SERVICE@ALLKEYSCOMPUTERGUYS.COM

Take Control Ebooks

The Answers You Need Now, from Leading Experts

AVAILABLE FOR ONE MONTH - GET IT NOW

by Karen Beal

Want to download a free eBook on how to use Dropbox?

Take Control (http://www.takecontrolbooks.com/) has allowed UKMUG to offer free copies of some of their many great books to our MUG members. All you need to do is go to the UKMUG website and download the book. Here is what they say about themselves: It's time for you to Take Control with highly practical, tightly focused ebooks covering all Apple devices. Written by the same expert authors responsible for best-selling print books but available much more quickly, Take Control ebooks provide the technical help you need now. Our ebooks use carefully designed layout and typography for easy onscreen reading, and they include bookmarks, clickable links, and an "Ebook Extras" link that lets you access free updates.

This month, we offer the follow full eBook, free for download, on our website:

Take Control of Dropbox

Whether you're already among the millions of people who sync and share files with Dropbox or you plan to join their ranks soon, this ebook will teach you about the many features—especially the non-obvious ones!—that make Dropbox an exceptionally popular Internet service.

Take a look through it - and let us know what you think, email Karen at kbeal1@aol.com. MU

iPhone Orientation

from J. D. Biersdorfer of The NY Times, submitted by Graham Thomas

If you keep your iPhone's orientation locked in portrait mode all the time, you miss out on features of certain apps in their horizontal landscape mode. For example, once you turn off the orientation lock (by swiping up from the bottom of the screen and tapping the lock icon in the iOS 7 Control Center) and allow the screen to rotate, the Calculator app transforms from a simple arithmetic interface in portrait mode to a scientific calculator for complex math formulas in landscape mode.

Rotating the Stocks app into landscape mode displays a much longer span of share prices for a selected stock and adds other features. Press one finger to the screen and drag it to see the share price on a specific day, or press two fingers to the screen and move them to see a stock's performance within the time span marked between your fingertips.

Spinning the iOS 7 Calendar app into landscape mode adds a weekly grid view of your schedule. Many landscape-mode features also work on the iPod Touch and on earlier versions of the iOS software.

And for those of you who are wondering how you can lock your screen orientation… Here's How:

1. How you begin depends on what version of the iOS you're running. In iOS 7, make sure Control Center is turned on and then swipe up from the bottom of the screen to reveal Control Center. In iOS 4-6, begin by double clicking the home button on the front center of the iPad or iPhone's face. This will bring up the process menu, listing your apps.
2. In iOS 7, look for the icon that shows a lock with a curved arrow around it. In iOS 4-6, slide the list of apps to the right. This should reveal the iPod app, iPod controls, and an icon with a circle-shaped arrow on it. This is the screen orientation lock.
3. Tap the orientation lock icon to lock the screen to its current position. Tap it again to unlock.
4. When you're done, single click the home button again to return to your apps. MU

From Take Control's Passwords book:

Tip: To test the entropy* of your passwords, you can try a free online tool called **zxcvbn**. Not only will it tell you a password's entropy in bits and the estimated time to crack it, it will also point out specific areas of weakness (such as dictionary words and patterns in the password). And don't worry, it does all this safely within your browser—it doesn't transmit your passwords over the Internet.

https://www.cygnius.net/snippets/passtest.html

**the word entropy means disorder, randomness, or unpredictability. Cryptographers use the term entropy to refer to a mathematical measurement of a password's complexity.*

Free iPhone User Guide download

submitted by Diane Marshall

Diane was looking for a little help figuring out the status icons on he iPhone when she ran into this free guide, chock full of all the stuff you need to know.

The status icons are on page 12.

http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf

Customize your laptop!

submitted by Karen Beal

Beautiful and fun Macbook decal stickers by HelloSkin on Etsy, for under $16:

http://tinyurl.com/k23lpr8

Apple praised for plan to undermine system that secretly tracks customers

by Craig Timberg, a national technology reporter for The Post, submitted by Lindi Mallison

As the political push to curb digital spying remains mired in debate, those who produce the technological wonders of our age are fixing on a more direct response: If you can't legislate privacy, build it in.

It is against this backdrop that many in the technological community are applauding the decision by Apple to tweak how the iPhone searches for WiFi connections. Through a relatively simple software update, the company plans to undermine a widely deployed system that stores such as Nordstrom have used to track the movements of customers to analyze shopping habits.

Tracking shoppers is not the same as tracking terrorism suspects, but software developers increasingly appreciate that all digital surveillance relies on access to data created whenever humans and computers interact. That has prompted a widespread rethinking of how computer systems are designed, with the goal of making data much harder for outsiders to vacuum up, be they intelligence services or the local mall.

In the aftermath of Edward Snowden's revelations about government surveillance, efforts began to extend encryption, repair long-standing security flaws in software and limit the amount of information that apps and Web sites "leak" — meaning inadvertently expose to unauthorized collection. Other developers began looking to build entirely new communications systems that are decentralized, making them inherently resistant to mass surveillance.

"The solutions here are going to be technical," said Christopher Soghoian, principal technologist for the American Civil Liberties Union. "The biggest and most enduring impact of Snowden is going to be the way the engineering community adjusts."

Apple, which declined to comment on its new WiFi system, plans to have iPhones and iPads send out random identification codes when they look for WiFi signals, according to information sent to app developers.

Once this change takes effect, probably in September, it will defeat systems that rely on a single, distinctive WiFi code to track shoppers by their iPhones, monitoring where they move in a store and when they return. The goal typically is to deliver coupons and collect data on shopping behavior. Other smartphones, including those using the popular Android operating system, will still be trackable through their WiFi signals.

Nordstrom once used such a system but stopped after public outcry. Euclid, one of several analytics companies that provides such services, does not name its customers but claims they include major retailers selling clothing, auto parts and housewares.

Apple does have its own system for delivering location-based advertising to customers, called iBeacon, but it requires that users opt in by opening a store's app on their smartphones. Services based on WiFi codes, by contrast, can operate without consent or the knowledge of customers, even when they are not using their phones. There are other technologies capable of tracking customers as well, though perhaps none is as simple and inexpensive for stores to use, experts say.

Privacy groups long have pushed for changes to WiFi technology to make location tracking more difficult. They also have pushed for end-to-end encryption of e-mail, social media postings and video chat, and for tech companies and judges to treat surveillance requests from investigators more skeptically.

Many privacy advocates have come to believe that even if the United States enacts new legal curbs, it would not be enough to restore user privacy in an era when the Chinese, Russian and Israeli intelligence services — not to mention countless criminal hackers — have powerful spying tools.

Such thinking has fueled a push by the volunteers who run Jabber, a popular instant-messaging technology, to institute new rules — long debated but never implemented — requiring that all users connect over encrypted links. That change took effect last month, after what amounted to a manifesto signed by more than 70 developers and operators of Jabber servers.

"We had been talking about this for years, but we needed a kick in the pants," said Peter Saint-Andre, who operates Jabber.org, a popular server.

A similar effort is underway to improve a popular form of encryption, TLS/SSL, that dates to the 1990s and has known weaknesses. A working group of cryptologists is searching for a way to harden the technology while adding new features.

People are taking seriously the need for encryption, even of data that seem innocuous, because of the ways it can be used.

In many cases, action has come from companies, such as Google, Facebook, Yahoo, Microsoft and Apple, that more often had been targets of criticism by privacy advocates because of how they collect and handle personal information.

"Apple hasn't been limiting the information that Apple can see and that Apple can gather," said Seth Schoen, a senior staff technologist for the Electronic Frontier Foundation, a civil liberties group in San Francisco. "They've been limiting what third parties can see." MU

iCloud Keychain - Pros & Cons

by Joe Kissell, author of the Take Control eBook

Mac OS X has always had a system-wide mechanism called Keychain for securely storing passwords and other private information, but until recently it didn't quite qualify as an all-purpose password manager. That changed somewhat with the introduction of OS X 10.9 Mavericks and iOS 7, both of which include a new feature called iCloud Keychain.

Enabling iCloud Keychain gives you a new keychain (called—you guessed it—iCloud), which initially contains most of the items from your existing login keychain, but which uses Apple's free iCloud service to sync across your devices. iCloud Keychain also gives Safari a random password generator; lets you store, sync, and fill credit card details; and erases the old limitation of one set of credentials per Web site.

My favorite thing about iCloud Keychain is that it provides autofill.

in Safari on iOS, something that can't be achieved in any other way due to Apple's sandboxing rules. And, because it integrates with OS X and iOS, it can also handle system-level passwords. For example, if you entered a Wi-Fi password on your Mac and later connect to the same network on your iPhone, you won't have to type in that password.

If you use only recent-vintage Apple devices, iCloud Keychain could conceivably be all the password manager you need. However, it's quite limited compared to some of the other password managers I discuss in my book. For example:

It can't sync with Macs running older versions of OS X, with iOS devices running iOS 6 or earlier, or with Windows or Android.

It currently works only in Safari.

Although it does create random passwords, they're all 15 characters long with the format XXX-XXX-XXX-XXX, where each X is an alphanumeric character (no symbols other than the hyphen are used). If you want a longer password or one with a more varied character set, you're on your own.

It can't store or enter a credit card CVV number, which most other password managers can do.

It won't help you with software licenses, secure notes, and other arbitrary data types.

By default, it locks only when your Mac or iOS device does, which strikes me as a poor balance between security and convenience.

(This fact also makes it that much more important that you choose an outstanding login password for your Mac!)

For these and other reasons, I use iCloud Keychain only as a supplement to a third-party password manager. (And yes, you can easily use both at the same time.)

To learn more about iCloud Keychain, read my Macworld article ***How to use iCloud Keychain*** (http://www.macworld.com/article/2058081/how-to-use-icloud-keychain.html) or my ebook ***Take Control of iCloud*** (http://www.takecontrolbooks.com/icloud). MU

How to Keep Data Out of Hackers' Hands

by Molly Wood for The New York Times, submitted by Jim Spencer

Hundreds of millions of email addresses and other types of personal identification found in the hands of Russian hackers. There are common sense steps everyone can take to keep the exposure to a minimum.

How do I know if my personal information was stolen?

Assume it is. The latest breach is huge, and similar attacks and smaller thefts are happening all the time. It is wisest to improve your online security immediately.

Should I change my password?

The first step, as always, is to change passwords for sites that contain sensitive information like financial, health or credit card data. Do not use the same password across multiple sites.

How do I create stronger passwords?

Try a password manager like LastPass or Password Safe. These sites create a unique password for each website you visit and store them in a database protected by a master password that you create. That sounds dangerous, but password managers reduce the risk of reused passwords or those that are easy to decode.

If you create your own passwords, make sure they are not based on dictionary words, which can be cracked relatively quickly. We suggest creating an anagram from a sentence, and using symbols and numbers to make it more complicated.

For example, the sentence One time in class I ate some glue could become 1TiC!AsG.

Create the strongest passwords for the sites that contain the most sensitive information and do not reuse them.

Are passwords enough?

Passwords are not enough. If a site offers additional security features like secondary or two-factor authentication, enable them. Many bank sites and major sites like Google and Apple offer two-factor authentication. In some cases, the second authentication is required only if you're logging in from a new computer.

How can I stop my information from being stolen?

You cannot. Regularly monitoring your financial records can help minimize the damage if someone gets your information. The companies storing your personal data are responsible for securing it. Consumers can slow down hackers and identity thieves, but corporate computer security and law enforcement are the biggest deterrents. MU

"Yesterday I changed everyone's password to 'password'. I sent it to everyone in a memo, put it on a big sign on the wall and printed it on all of the coffee cups. Guess how many people called me this morning because they forgot the password."

PrintSource of the Keys

Color Copies • Large or Small Orders

Rack Cards • Business Forms & Checks • Brochures

Business Cards • Letterhead • Envelopes

Signs and Banners • Multi-Part Forms • RX pads

Posters • Rubber Stamps • Graphic Design

305-664-1002

81933 Overseas Hwy., Islamorada

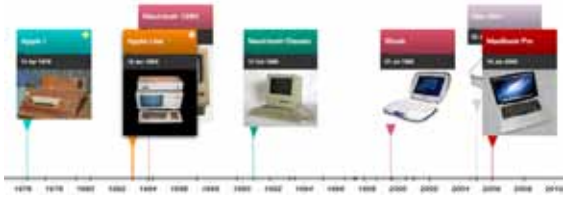
printsourcekeys@yahoo.com

Timeline... 37 years of Apple Computers

submitted by Graham Thomas

Check it out, at:

http://histropedia.uat.co/Home.aspx?vz1ndyv56m#.U-jIn5J4cPs.email



dummies.com

is a great place for useful and brief Mac Tips and Tricks! Check it out!

MU Classifieds • MU Classifieds

Got Stuff for Sale or Giveaway?
Need Something?
Email ukmug@bellsouth.net

VISIT TODAY!

http://ukmug.pbworks.com/

Post questions and requests for help
Post tips and tricks
Post your favorite links
Check on upcoming meetings
Download our newsletters & more!

Come at 6:30 for the Beginners Circle:

Bring your laptop and your questions at 6:30, and for a half-hour prior to the main meeting we'll have experienced folks available to help, one on one, or in small groups.

FREE CLASSES

The Apple Store at the Falls has free classes every Saturday! They also have one-on-one training, workshops and the Genius Bar. Call or check the web for more info:

Apple Store at The Falls
305-234-4565
8888 SW 136th Street
Miami, FL 33176
Mon-Sat:10-9:30pm
Sun: noon-7pm

http://www.apple.com/retail/thefalls

Tom Stack & Associates, Inc.
154 Tequesta St.
Tavernier, FL 33070
305-852-5520
www.tomstackphoto.com

We are pleased to announce our New Epson 9880 44" Printer with Vivid Magenta Technology. For all UKMUG Members we offer 20% off Printing Prices. We also offer photo restoration, as well as Stock Photograpy for your web site.

OUR LINKS ARE LIVE!

If you haven't figured it out yet, try it. Click on any blue, underlined link in our Macaholics Unanimous newsletter and it will take you to the web.

Did you see that picture of you, taken at the last meeting?

http://ukmug.pbworks.com/

Monroe County Recycling Collection Center:

MM 100.1 Oceanside (Magnolia St.)

453-0788

E-RECYCLING: 2nd & 4th Wed. every month, 10am - 2pm

E-waste: Monitors & Computers Batteries, Televisions, All Telephones & FAX Machines, Printers / Copiers, DVD / VCR Players, Radios & Speakers, Discs & Cassettes
Also taking Hazardous Household Waste.

Macaholics UNANIMOUS

is the official newsletter of the

Upper Keys Mac Users Group

A nonprofit organization devoted to the use (and sometimes abuse) of the Macintosh computer. Subscriptions are free. Contents © 1993 - 2014 by the Upper Keys Macintosh Users Group except where noted. All other rights reserved.

219 Second St. • Key Largo FL 33037
(305) 451-4601 • ukmug@bellsouth.net

Share! Send us your stuff!

Get organized today with TopXNotes™ - the premier Personal Note Manager for Mac.
Top rated by Charles Moore, Macsimum News, The Macintosh Guild, and Macworld Magazine.

Create, View, Access and Organize Your Notes

Loaded with handy features!

- Quickly create, access, update and categorize notes
- View multiple notes at once
- Fast access to your notes with QuickNotes™
- Simple import and export; drag and drop support
- Encryption for sensitive information
- Customizable templates included

Award Winning Software for your Mac

Tropical Software WWW.TROPIC4.COM Macworld TopXNotes® Personal Note Manager