

# KeyMac Journal

Volume 10, Number 6

June, 2006

## President's Message

AppleCare is that big question we face every time we buy a new Mac—several hundred bucks more on top of an expense you may already have a bit of trouble justifying.

I never used to buy it. My first Apple was a II in 1981, and my first Mac was in 1985. In the summer of 2003 or 2004 I first bought the protection with my G4 tower. I repeated the AppleCare purchase last August when I bought my G5 20-inch iMac. The sales guy at Small Dog Electronics, whom I have grown to trust, recommended it unhesitatingly.

Tonight—Wednesday, June 14—was the first time I have ever used the AppleCare help line. At about 8:30 p.m. my screen froze and I had to crash out. Then the start-up chime never sounded and the fan went to high speed and would not cut off. The screen remained black the entire time.

The hold on the call to AppleCare was a modest five minutes and the guy might have been Canadian, but not Far Eastern. He had a good bedside manner and had me perform all the resets that we could—all to no avail. Then he determined that Greenville CompUSA would be my destination tomorrow morning.

I'll let you know how this works out at the meeting on Tuesday. The way it sounds, I will have my payback for the last two AppleCare purchases soon.

*Gene*



## MONTHLY PROGRAMS

**June 20:** Q & A time with Alan Houtzer. If time permits Gene may be able to give us an introduction to the Microsoft Office program.

**July:** VACATION TIME—NO MEETING  
NO JOURNAL

Please mark your calendar. Our monthly programs are the third Tuesday of the month, beginning at 10 a.m. at the Activity Center and usually lasting until noon with a short refreshment break.

## OS X DISCUSSION GROUP

**August 1:** An informal gathering of members where questions are answered and problems solved—members helping members. All are welcome. The schedule for the year is:

**Tuesday, August 1**  
**Tuesday, September 6**  
**Tuesday, October 4**  
**Tuesday, November 1**

**MASTHEAD**

Published by the KeyMac Computer Club

Co-President.....Bob Beaupre  
[spyglass25@mindspring.com](mailto:spyglass25@mindspring.com)  
 Co-President.....Gene Madill  
[madillg@bellsouth.net](mailto:madillg@bellsouth.net)  
 V.President.....Drake Hawkins  
[drakhawk@earthlink.net](mailto:drakhawk@earthlink.net)  
 Co-Secretary.....Joan Englehart  
[joaneng@bellsouth.net](mailto:joaneng@bellsouth.net)  
 Co-Secretary.....Margret Nordquist  
[margret061836@bellsouth.net](mailto:margret061836@bellsouth.net)  
 Treasurer.....Arlene Stanicek  
[astan01@bellsouth.net](mailto:astan01@bellsouth.net)  
 Co-Editor.....Gladys Calhoun  
[gladyscalhoun@earthlink.net](mailto:gladyscalhoun@earthlink.net)  
 Co-Editor.....Joan Englehart  
[joaneng@bellsouth.net](mailto:joaneng@bellsouth.net)  
 Librarian.....Al Kishbaugh  
[kish12@earthlink.net](mailto:kish12@earthlink.net)

themselves. They may send copies of themselves to other computers through email or Internet Relay Chat (IRC).

**What is a Trojan Horse?** A Trojan horse program is a malicious program that pretends to be a benign application; a Trojan horse program purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but Trojan horse programs can be just as destructive.

**What is Spyware?** Spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, often for marketing purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits the information in the background to someone else. □

**Phishing Around  
 Don Mayer, Kibbles & Bytes**

**Treasurer's Report**

Balance May 7, 2006	\$1449.99
Withdrawals	
Gift & Refreshments	107.78
Deposits:	
Dues	85.00
Interest:	.64
Balance June 7, 2006	\$1427.85

The biggest email scam around these days is phishing. "Phishing" (also known as "carding" and spoofing") refers to email that attempts to fraudulently acquire personal information from you, such as your account password or credit card information. On the surface, the email may appear to be from a legitimate company or individual, but it's not. The crooks are getting more and more sophisticated with their phishing messages and if you are not careful, you might get caught!

Most phishing attempts use credit card-issuing banks, ebay, Paypal, or Amazon, but I have seen phishing emails that appear on the surface to come from obscure companies. Your safe computing rule should be to never send credit card information, account passwords, or extensive personal information in an email unless you can verify that the recipient is correctly identified. Many companies have policies that state they will never solicit such information from customers by email. It is a very rare company that will ask for this information without surefire identification.

**COMPUTER SECURITY**

This month's issue of the *KeyMac Journal* concentrates on information and tips addressing possible challenges to the safety and privacy of our computer files.

**Glossary**

**What is a Virus?** A virus is a manmade program or piece of code that causes an unexpected, usually negative, event. Viruses are often disguised games or images with provocative marketing titles.

**What is a Worm?** Computer worms are viruses that reside in the active memory of a computer and duplicate

If you do get email that you think is a phishing scheme, here are some tips that can help you determine its legitimacy:

- 1. Find out where the mail is from:**  
 View the email headers to see where the message really originated from. If you are using Mac OS X Mail you can view "long headers" by going under the "View"

menu item, choosing "Message" and then the subcategory "Long Headers." This will give you complete information about the origin of the email.

A typical email header displays several lines that begin with "Received." Note the last "Received" line; this line will look something like this:

```
Received from yourtypicalwebsite.org  
(123.456.789.101)
```

If the "Received from" information does not match the email address of the sender or the company being represented in the email, it usually means that the message did not truly come from that individual or company. So if your message is from Wells Fargo and you do not see a Wells Fargo address in the last "Received" line, there's a good chance this is a phishing scam and should end up in your deleted mail.

## 2. Watch out for embedded links:

One common phishing technique is to include links in an email that look like they go to a legitimate website. However, upon closer inspection, the link may actually take you to a website that has nothing to do with the company the email is pretending to be from, even though the resulting counterfeit website may be designed to look exactly the same. Do not believe your eyes. Look at the real address of where you have surfed if you accidentally click on that link. You will see that it usually has nothing that would identify it as belonging to the merchant.

In MacOS X 10.4, Mail can help identify these type of links. Simply mouse over (but don't click) any link in an email, and you will see a pop-up that shows you the actual URL that you will be taken to.

## Top 8 OS X Safety Tips by Aaron Wright

There was a little speculation recently that McAfee, a dedicated security company, had unnecessarily worried people into buying its products with the news that, from 2003 to 2005, the number of vulnerabilities discovered on the OS X platform had increased substantially, whereas Windows vulnerabilities discovered in the same time period had increased only slightly. To the blind-sighted or Mac newcomers, this is a worrisome fact, but the truth is being bent—quite a bit.

It is probably true that the number of vulnerabilities in OS X have increased, but it's also clear that those

vulnerabilities are quite minor when compared to the Windows threats. It's nothing that should really worry people, as the truth is being blown completely out of proportion just to increase sales of McAfee software.

However, I do think it is important that Mac users not be arrogant about the whole matter of OS X being "virus" free, because we will be hit by a large virus. It's just a matter of time.

So what steps should people be taking in order to protect themselves further?

### 1. Get some Anti-Virus software

There's no real need for this at the minute, but if you want to be extra safe, some anti-virus software isn't going to be amiss. McAfee has just recently announced its Virex anti-virus software turning Universal.

Norton also has an anti-virus program for the Mac platform that is currently in its tenth edition and has also recently turned Universal.

While the amounts of threats to OS X are few-to-none, you should bear in mind a few things. There are a large number of Word and Excel viruses on the Office platform that affect both Windows and Mac users, thus, threatening Mac users. There's also the unknowing threat of a virus outbreak occurring right out of the blue, which is not likely to happen, but not impossible.

### 2. Turn that Firewall on

Although the thought of some Spyware creeping into your system and some important information of yours being transmitted outbound, or the idea that you might be getting spied upon by someone close to you are all horrid (and unlikely at the moment), they are possible.

The Firewall, which is both off by default and difficult to find for new Mac owners, should be turned on before you connect to the Internet.

The easiest way to turn it on from your desktop is to direct yourself to Spotlight, type in "Firewall," and then click on the search result "Sharing" that will open the Sharing pane in the System Preferences. You will find the Firewall located there. Turn it on and lock the keypad at the bottom to stop it from accidentally being turned off. You may want to check which services you wish to allow your Firewall to use without causing a disturbance. Most of the time, you won't need to turn any on, especially if you're a home user only.

### 3. Services

You'll notice in the Sharing pane that there are three tabs: Services, Firewall and Internet. We've just dealt

with the Firewall. It's also an idea to check out which services are active. Services are the ports (or 'Doors') to your computer as seen from the Internet or local area network. When a service is turned on, you're opening one of those doors to allow someone (or something) to access it. Although it might sound risky, they are useful, especially if you're part of a network, but if you don't know what they are or how they are used, you're putting yourself at risk. To be safe, keep them all off.

#### 4. FileVault

If you've ever browsed through your system, you may have come across something called FileVault, which is exactly as it sounds, a vault for storing all of your files. The FileVault (open as you did with the Firewall) uses the latest government security standard called AES-128 encryption and helps safeguard your files. It encrypts and decrypts on the fly (as you're working) and all without your knowledge. FileVault can protect prying eyes from files such as your banking details, private letters or even family photographs using a password—set up by you—an excellent way to give you peace of mind when using your Macintosh system.

#### 5. Keychain pop-ups

Ever been asked something when using Safari regarding a keychain? All the usernames and passwords you use throughout your system are stored there and are only accessed when the system asks you to enter the administrator password. In short, it keeps all your passwords in one safe place, away from prying eyes and harmful Spyware.

#### 6. What else you can do

There are a few other ways of protecting yourself when you're on a network or the Internet, some of which are a little too "over-kill," especially if you're a new Mac user. However, there are a couple of last steps you can take, on top of everything I've mentioned above, to keep yourself extra safe.

In Safari, turn off the option to automatically open downloads when completed. To do this, open up Safari, click on "Safari > Preferences" and then under the "General" tab, untick "Open 'safe' files after downloading." Although Safari will never open an unsafe file, it's only so smart and can never know for sure if a file is definitely safe. By turning this off, you're also turning off the likelihood of a virus trying to open itself after being downloaded.

#### 7. Keep cookies restricted

Think of cookies as a token-pass. Every time you visit a website, you're issued a token so that your computer knows you've been there before. They're quite useful

because they store some basic information that helps to speed things up when browsing the Internet. However, some websites like to give you tokens with tracking-beacons in them, and whenever you go about your business on the Internet, your tracking-beacon is sending information back to the website it originally came from. It's never nice to be spied upon, so keep your cookies restricted. To do this in Safari, go to "Safari > Preferences," click on the "Security" tab and then select one of three options under "Accept Cookies." I usually keep mine set at "Only from sites you navigate to" because I know that these are safe.

Apple is always working around the clock to find more holes in the system. Your Mac auto-updates itself by default, but it's always best on occasion to double check that there are no more updates available by using the Software Update, which can be found underneath the Apple (top left in menu bar). Any security patches that need to be installed on your system will be accomplished via Software Update.

#### 8. Being smart

The easiest, cheapest and most reliable way to keep yourself safe from Internet-baddies is to use a bit of common sense when surfing the web or reading emails. Never click on a link that claims to offer you free junk, especially if it asks for your details such as email address or name. If you ever receive an email that claims to be from your bank, read it with an open mind and be careful. If they should ask you to enter any details, it's likely to be an act of Phishing (*see separate article on Phishing elsewhere in this issue*).

The last thing to be careful with is your passwords. Whether you're buying something from the Internet, logging into your email, checking Internet banking, or even installing something on your computer, you'll always be asked for a username and password. Be smart with this. Always include uppercase and lowercase letters, numbers and possibly an underscore or two in your username and passwords to make life a lot harder for a thieving hacker. Also be sure to set a username that doesn't easily identify who you are and a password that has no relevance to your username.

None of these ideas will ever fully guarantee that you are safe from harm on the Internet, but with all of these precautions combined, you will be safe enough to use your computer with peace of mind. □

#### QUOTE OF THE MONTH

*Treat your password like your toothbrush. Don't let anybody else use it, and get a new one every six months.*  
(Clifford Stoll) □