

Apple Bytes

The Newsletter of the **Lynchburg Apple Core**

Volume 2005.9 ----- Lynchburg, VA ----- September 10, 2005

September Meeting

General meeting is at Lynchburg College, Thursday, September 15, 7:00 PM.

Mac Security will be the main topic of discussion at the regular meeting at **Lynchburg College, Hopwood Hall** which will begin with a Q&A session at 7:00 PM and the program at 7:30 PM.

~ ~ ~ ~ ~

CVCC Mac OS X Class September 30, October 1, 7, and 8

The Lynchburg Apple Core is sponsoring a 1-credit college class on Mac OS X, covering both Version 10.4 Tiger and Version 10.3 Panther. This class is intended both for Mac users who are new to OS X and those who have been using it for some time but who want to gain a better understanding and become more proficient in the use of their Macs. The class will be relatively small and will be geared for a lot of personal attention, questions and answers. It will include coverage of iPhoto, iTunes, iMovie, iDVD, GarageBand, Safari, Mail, and AppleWorks.

This is a weekend class, September 30, October 1, 7, and 8. Two Friday nights from 5:30 PM to 9:00 PM, and the two Saturdays from 8:00 AM to Noon, to minimize disruption of your normal schedules. Gordon Mattox is the instructor. It is listed as Business 195-01MD, "Macintosh Operations - Mac OS X". Sign up through the CVCC Admissions Office on campus, or if you have been registered before, call 832-7633. Or call Gordon at 401-0163 for more info. **Please note, the class will be canceled if there are not enough registrants!**

~ ~ ~ ~ ~

How Safe is Your Mac - Really?

- Gordon Mattox

The subject for this month's discussion was suggested by some of the responses received from the program survey done at last November's annual dinner. The survey item titled "Protect Your Privacy" came in as Number 6. I'm sure this means different things to different people, but some things we have all talked about from time to time are viruses, hackers, and other aspects of safe computer operations on our Macs.

The March 2005 issue of Macworld magazine had a feature article entitled "Mac Security. Fact and Fiction" with the subtitle "Viruses, Spyware, Internet Hackers, and Wireless Prowlers." The issue also included "Mac Attacks", "Select Your Shield", "Raise the Wall", "8 Ways to Protect Your Mac Right Now", and "The Key to Your Mac." All-in-all, it was ten pages of good information which can't all be covered here. It's intended that this month's meeting cover various aspects of these topics and all are encouraged to ask questions and join in the discussion.

Fact and Fiction - From the Macworld article

Mac Users don't need to worry about viruses. Macworld says "False" and discusses why they do. They say "If there is a virus attack, those of us who have good, up-to-date antivirus software installed will have the best odds of escaping unscathed." Macworld rated the four antivirus programs and only one got above a 3-mouse rating, 4-mice, Intego's **VirusBarrier X 10.1.1**, and said it sells for \$60. At the Intego site, it sells for \$69.95. Then you have to

subscribe for the periodic updates at \$25 per year. At least one user report at VersionTracker could not detect any real updates even though he had subscribed. VersionTracker compiled a 3-mouse rating from user feedback.

Another anti-virus program is McAfee's **Virex**. For some time, Apple offered a free copy of Virex with each Dot Mac subscription, but dropped it when Mac OS X 10.4 "Tiger" was released, because Virex was not compatible with Tiger. McAfee has since updated Virex but Apple has not yet reinstated the free copy, and may not do so in the future.

This is a controversial topic and there are voices on both sides of the debate. But one of my favorites is from David Pogue, author of Mac OS X, the Missing Manual who said, "Viruses? What viruses?" Another was from a Mac "blogger" on SlashDot who titled an entry "Virex is the Virus!"

As of this date, there are no reported viruses in Mac OS

In summary, I personally do not worry about viruses on the Mac and I'll tell you why at the meeting.

You're vulnerable to Windows viruses if you run emulation software. True, and I agree, but it's easy to manage the potential here. You can only get a Windows virus if your Windows environment comes in contact with the outside world via an internet connection or via an infected PC disk used in the Windows environment. The virus, if you get one, will only affect the Windows virtual disk.

Mac users don't need to worry about spyware. True. But there are currently no real spyware programs that affect the Mac. But in OS X, for any program to be installed, whether it's a keystroke recorder (spyware), a Trojan Horse, or a virus, it must have permission to install from an Administrative user -you. So really, you are the first-line best defense for your computer.

Sending chat messages is akin to throwing paper notes across a crowded classroom. True. Whether you are using iChat, AOL Instant Messenger (AIM) or MSN Messenger, your information can be picked up by someone watching your network traffic. So, the action here is, watch what you do when you're in this mode.

When I'm using a wireless network at home, I'm perfectly safe. True and False. The wireless protocols 802.11b and 802.11g have limited range, and so your first layer of protection is that fact. The next is to make certain of your security settings when you set up your network, such as setting your WEP password, etc.

When I'm using a public hotspot, all of my passwords are being stolen. True. It's not literally true, but the potential is so high you might as well assume the worst. But the solutions are beyond the scope of this discussion here. Just be careful what you do when you are using a public hotspot.

The Mac's default security settings are all you need to protect your computer from hacker attacks. False. The first thing to do is to open System Preferences and go to *Sharing* and click on the middle button of the bar near the top "Firewall" and turn the firewall on. In the window below that Firewall "Start" button (now it says "Stop"), you see a list of services that operate through communication "ports" in your operating system. These ports are all closed until you open them to allow those network communications. For security sake, keep them closed unless you need to open them to do the things on the network that you want to do.

Eight Ways to Protect your Mac Right Now - *From the Macworld article*

- 1) Turn off automatic login.
- 2) Require a password for waking your Mac from sleep or a screen saver.
- 3) Lock your keychain.
- 4) Change your keychain password.

5) Store your sensitive files in an encrypted disk image.

6) Completely erase sensitive files.

7) Use Filevault.

8) Set an Open Firmware password.

We'll talk more about each of these procedures at the meeting.

**September Meeting:
Lynchburg College, Hopwood Hall - Thursday October 20, - 7:00 PM
Build a Web Site**

A Note From **Tony Young**

I have just become involved with a truly compassionate and honest online provider. It is called Carrot Ink at <http://www.carrotink.com/> and they are located in Texas. On calling them toll-free at 877-322-7768 I spoke to some very nice people, very eager to assist. The company is called Carrot Ink and it can provide ink for all of our printers at a very reasonable price. The set for my printer cost \$43.95 as compared to the standard price of \$88.95. I ordered all four colors for my Epson C86 Printer and received the package in a couple of days. I installed the cartridges, but one of the would not work, Calling them back they issued four more for me and told me to return originals in a postage free box. Unfortunately the black on did not fit (some Epson Printers are "picky") and are old so they sent another Black.

These girls have been very helpful and obliging and spare no effort to please customers.

They can be located at the above number and or www.carrotink.com. If you are not completely satisfied, ALL items can be returned and a refund is cheerfully returned. - *Tony Young*

Apple Bytes, the monthly newsletter of the Lynchburg Apple Core is delivered via e-mail and is available as a downloadable PDF at <http://www.lyncburgapplecore.org>. Please send your comments and questions to Program Chairman & Newsletter Editor Tom Johnson at graystranger@earthlink.net, or President Gordon Mattox at gcmattox@mac.com.