

# California Computer Care

News,  
Views,  
Tips and  
Cool Techniques  
for CCC Members

March 2006  
Vol. IX, No. 3

We  
speak  
Geek,  
so you  
don't  
have to.

## Mac Security Today

Ooooo! Scary...

Not really. The Geek-to-Geek discussion of Mac computer security recently caught the attention of the mainstream press. And, as usual, the mainstream press has misunderstood and mis-reported virtually everything about the issue.

*There is no threat.* Mac users are still as safe from security threats today as we have been for the last six years. You still do not need anti-virus software (there are no viruses) or anti-spyware software (there is no spyware). Even the most rabid security experts agree, reluctantly, that Mac users are safe from harm (see Winn Schwartau's web site: <http://www.securityawareness.blogspot.com>). But, this may change someday.

Of course, that has always been true: *Things change.* And, as a corollary, the future is unpredictable. What you need to do about the possibility of future security threats is noted in the March tip on page 2. For now, some background on Mac security and why the mainstream press is all worked up.

*Proof of Concept.* One of the things that computer security experts get paid to do is devise new ways to attack computers. When a new attack is developed, it is shared with other experts so that counter measures can be created. A security expert's new attack is called a *Proof of Concept*.

Several *Proof of Concept* attacks against Mac OS X have been created. As of yet, none has been tried except experimentally. No bad guys have stumbled upon these techniques or created others that the security experts don't know about.

However, each *Proof of Concept* has sparked many news stories about lack of security in Mac OS X. Where do reporters get their information about these new security threats (usually mischaracterized as "*viruses*")? In

every case the source of these stories is one of the big anti-virus software publishers (*Symantec* and *Sophos* seem to be the most prominent sources). So, you see, since there are no viruses, worms or trojan horses that can attack Mac OS X, the anti-virus software publishers have nothing *useful* to sell to Mac users. It is in their best interests to drum up hysteria about theoretical threats.

*Security threats come in four types.* The best known are viruses. Viruses are applications that invade and take control of other software (like real viruses do to cells in your nose to give you the sniffles). Viruses spread when folks copy them to their hard drives and run them. Because they are applications (just as *iTunes* and *AppleWorks* are), when viruses are first run, Mac OS X is suspicious of them and asks the user (that's you) to authorize the action by demanding your *User Name* and *Password*. If you do not authorize the virus, it can't run, and no harm is done.

Worms are the second category of threat. Worms cause problems like viruses, but they have the added ability of being able to travel, on their own accord, over computer networks, infecting each computer that they find. Mac OS X has several levels of protection against worms. This protection is so good that no one has been able to devise a functional *Proof of Concept* worm.

Almost all *Proof of Concept* threats have been trojan horses. Trojan horses are virus-like applications that masquerade as something else. The trojan horse might look like an MP3 music file or a JPEG picture file. The point of a trojan horse is to fool people into installing and running dangerous software in the belief that they are doing something else. The danger is that the user will absentmindedly enter their authorizing *User Name* and *Password* because they know that real MP3 and JPEG files are harmless. Once installed

all manner of mischief is possible. Real data files (documents, music, pictures, movies, etc.) will *never* require authorization. If one asks, always deny.

The fourth security issue has to do with allowing someone else to take control of your Mac without your knowledge. This can be done crudely by someone slipping into your chair when you've stepped away. Or, on a more sophisticated level, by someone burrowing in through a network connection such as your internet connection.

Mac OS X has been devised to make this extremely difficult to do, but because software is enormously complex, new dangers are unfortunately sometimes found. Apple is always on the lookout for these "security exploits" and issues fixes for them almost as fast as they are found. If you check *Software Update* and see *Security Updates* listed, these are fixes for flaws in Mac OS X.

The average Mac user, however, is not threatened by these dangers. The average user does not have their Mac set to allow outsiders to connect in any way. This makes your Mac as close to impregnable as it could possibly be. As such, you have no real need for these *Security Updates* and can ignore them.

Recently, a news story hit the headlines about a contest. The contest was a challenge to break into (crack) a Mac running Mac OS X and take control of it in any way. The *hacker* that won the contest, triumphantly claimed to have done so in less than 30 minutes.

But, the contest was bogus (something the technically ignorant reporters didn't realize). The contestants were given user accounts on the target Mac. With a user account, a hacker is no different than a person literally sitting at the Mac with one hand on the keyboard and the other hand on the mouse. Breaking in for such a user is a trivial task. When the challenge was repeated with a properly set up Mac, even though that poor machine was pounded mercilessly for a day and a half by hackers from all over the world, no one could harm it.

Here's a telling irony about security in the larger computer world. The valid test, which was run by Dave Schroder, a systems engineer at the *University of Wisconsin*, was cut short after only 38 hours because the university was afraid that the attacks against the test *Mac mini* would cause frustrated hackers to target the university's Microsoft Windows machines, since they are an easy target for any hacker bad guy.

## March Tip—

How to stay safe using your Mac:

- 1) **Don't turn on unnecessary services.** The *Sharing* system preference allows you to turn on File Sharing, Web Sharing, iTunes Sharing and more. Leave these turned off if you don't actually use them.
- 2) **Turn on your Firewall.** In the *Sharing* system preference is a firewall option. If it is off, turn it on. The firewall will make it nearly impossible for the bad guys to get at your Mac through your network or the internet.
- 3) **Be suspicious.** If you download an email attachment, a file from the internet or a file from another computer, assume that it is dangerous. Only open downloaded files from people and web sites that you know and trust.
- 4) **Don't trust your Mac's requests.** If a *User Name* and *Password* request dialog box pops up and you don't know why or understand what it is asking, DON'T give it your *User Name* and *Password*. Make a note of exactly what the dialog box says, cancel it and email the message to me. I will be glad to tell you if it is a safe request or not.

California Computer Care

P.O. Box 9445

Santa Rosa, CA 95405

(800) 540-8989

help@calcompcare.com

Like an  
auto club  
for your  
computer.