



MAC FACTS

from

Mac Help Desk

SUPPORT, SALES, TRAINING & SERVICE

(972) 783-9787 • (214) 249-9543 - *Pager*

e-mail address - machelpdesk@comcast.net

Web site - <http://www.machelpdesk.com>

a Macintosh Solutions Provider company

Volume 13 Number 10

October 2003

A Message from Dru

As we move from the fall to winter, it's time to start celebrating the Winter Festivals. This month we start *Ramadan*, the month of Muslim fasting (<http://www.holidays.net/ramadan/story.htm>). And at month's end, we have Halloween (<http://www.holidays.net/halloween/story.htm>). But wait!...it gets better...☺

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

Having a holiday party at your home or office? How's about 'live' music? My band, LoveSong, can be had for just about a song. Call me at the office at 972-783-9787 for details. Don't dally, there's not much time left! Go here - <http://www.machelpdesk.com/lovesong/demo.htm> to hear a preview of our upcoming CD, *Promise Me Moonlight*.

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

The Apple Corps of Dallas' next meeting will be on October 18th at the Richardson Civic Center at Arapaho & Central Expressway. Go to <http://www.acd.org> for more info.

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

All those of you who aren't making enough money...raise your hands! I have work for y'all at our sister company, **the Richman group**. Call me at 972-783-9790 for more info.

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

Help! Help! Help! I'm about to be "arrested"! I've been secretly informed by the Muscular Dystrophy Association (MDA – Jerry's Kids, you know!) that I'm to be incarcerated at the Cappuccio Restaurant in Richardson on Wednesday, November 12th, unless I can raise \$2,000 "bail" in donations to MDA. If just a few of you would join me in donating \$20 (or more) I'll be assured that my stay in the "pokey" will be short lived. Send me an e-mail with your pledge. And thanks from me, and all of Jerry's Kids.



□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □



Is OS X Secure? Tips To Help You Secure Your Mac

Worms flood the internet, but is it only Windows users that have this problem?

With everything in the news lately about Microsoft machines being infiltrated by viruses and worms, several questions keep coming up in the tech community which we will address in this article.

1. Is it just MS computers that have to worry about having their security compromised?
2. Are Macs vulnerable to viruses, Trojan (horses), and worms (oh my!)?
3. What steps can I take to help keep my Mac from suffering from security problems?

Let's start with question number 1 –

Is it just MS computers that have to worry about having their security compromised?

The short answer is No, all systems have to worry. MS is more vulnerable out of the box, but even MS machines can be made more secure than they are when first set up using their default settings. MS has always been less secure than *nix systems for a number of reasons, which I will list below.

Closed source code: Some will argue that this makes things more secure, but all it really means is there are less people working on making it secure. If you have a dept of 100 programmers working on a project and they are the only ones who know how the internals work, then they are the only ones who can fix holes or possibly see where security flaws may exist and need fixing. However, look at open source projects, which often have hundreds or thousands of coders proactively working to keep it up to date, more efficient and secure. More coders = better chance for heightened security.

Slow uptake when alerted to security holes: When security people and/or hackers tell MS that they have found a security hole that needs fixed, MS will often put off fixing it until there is enough corporate complaints that the hole(s) need to be fixed. I have personally watched this happen several times over the last 5 years. Not a very proactive approach to security. Most experts tell the vendor about holes in their security long before they release the news to the public.

Hackers will keep hacking: Hackers will always keep poking at systems and software. They will find holes. If your software vendor is not proactive in patching/correcting these holes, then there will be breaches.

*MS is the *Evil Empire*:* I am not making a statement of fact or even my opinion, although I personally agree, what I am stating is the general feelings that seem to be prevalent in the computer using world. And because of this, they will be picked on and probed more often. And seeing as they are being used in so many commerce and infrastructure arenas, they should be.

The above are only a few observations I have made over the years

Now to question number 2 –

Are Macs vulnerable to viruses, worms, etc...?

Of course they are. All computer systems are vulnerable to these problems. Maybe not to a given variant or specific worm, virus, Trojan horses or whatever, but the potential is still there and always will be. The people who write malicious code will keep doing it and it is only a matter of time until they start aiming it at OS X. There were actually quite a few such programs aimed at Mac OS 9 and below, so they will come. There are a lot less pieces of malicious code written that affect Macs than there are WinTel machines, but the same is true of Linux and the Mac OS X's big brother *BSD, but there are some and there will be more in the future. Be conscious of this and keep your boxes moderately secure and you have a lot less to worry about.

Let's look at question number 3 now –

What steps can I take to help keep my Mac from suffering security problems?

There are several basic things which you can do to help keep your Mac OS X box more secure. Let's start with your connection to the internet. If you are connected directly to a broadband connection (i.e. cable modem, DSL or satellite) then go buy a router/switch. This is a good idea anyway if you want to have more than one computer on your connection. And yes, I know that you could use internet connection sharing, but using a router/switch is a lot better for the below reasons.

All machines have a direct link to your gateway. Therefore you are not taxing any machines resources by using it as a gateway machine

You basically get a cheap internal network. Therefore the internet only sees what you want it to see on your computers.

You can block ports network wide or forward ports to a specific machine. This can come in handy for running servers or using services.

It is a lot harder to breach a closed router than it is for some script kiddie to attack a machine that is connected directly to the internet.

As a side note, do NOT put your machines in the routers DMZ (by default no machines should be in the DMZ anyway). DMZ means demilitarized zone and is exactly what it sounds like. It places the machine in a position where it can be fully seen from outside your network as well as inside. This could be a big security hole.

Next, turn off services that you do not use. If you open your System Preferences and go to sharing, you have several options (which, by the way, all come turned off by default) and make sure there is nothing turned on that you are not using. Leaving services turned on could potentially lead to having someone break into your system.

Next, keep up on software updates and patches. If the software is distributed by Apple and it has a needed update, it will usually pop up in the software update. When it does, install the update, don't keep putting it off with "I'll do it later." or "When I have more time I will run the updates.", this leads to security holes. If you have 3rd party services or servers running on your Mac, check their sites regularly for updates or if it is available, sign up for a mailing list for that software product that sends news and alerts. And, just like with Apple distributed software, keep up on patches for third party software as well. Finally, make sure your firewall is turned on. OS X ships with a firewall by default and basic settings on it are easy to set up. To turn on your firewall, open the System Preferences and go to the Sharing pane. This pane has a firewall tab on it. Select this tab and if it does not say Firewall On, then click the Start button. You can add services that are allowed via the simple list and buttons below. Just select new and if your service is in the list, select it and enter its port number. If your service is not available, choose Other from the list. Choosing Other will give you, in addition to the Port field, a description field so that you can add a name for the service you

are allowing. So, say you want to install a Servlet/JSP server on your box, like Tomcat or Resin. After you have installed it, you can only access it locally because of the firewall, so to allow others to access it, go to your firewall settings and choose New, then select Other. In the Port field, put in 8080 and in the Description field, put in the services name, in my case, Resin. Click the OK button and the service is now allowed to get connections from other machines. The above example assumes that the Servlet Engine would be on the default port of 8080.

And finally, to close on the basic things you can do, Make Sure you have an Up To Date Anti-Virus installed on your box. This is something a lot of you are going to read and go, jeez, doesn't everyone have an AV running on their system? But the truth of the matter is, the majority of people do not even have an AV program installed, more less up to date. This is important. And right up there with it belong the following: Keep your Anti-Virus definitions Current and Scan files you download Before opening them.

These are just some of the basics of keeping your Mac OS X box fairly secure. Follow the above steps and you are highly unlikely to ever have a security breach on you system. This does not mean it could not happen, but more than likely will not as most security breaches are made by script kiddies who only know how to use the tools they download and when those tools fail on your box, they will move on to trying to find an easier box to crack.

□□□□□□□□ □□□□□□

NEWSLINE

Apple announced Windows support for iTunes, with a revamped iTunes Music Store and iPod Software 2.1 for Mac and Windows platforms. Apple said that it would offer more than 400,000 musical selections by the end of the month from "all five major music companies and over 200 independent music labels."

Apple also introduced two iPod accessories from Belkin, the \$49.95 iPod Voice Recorder and the \$99 iPod Media Reader .

An alliance with America Online, meanwhile, aims to expand iTunes's reach:

Apple and America Online, Inc., the world's leading interactive services company, today announced an alliance to provide instant, one-click registration to the iTunes Music Store for AOL's more than 25 million U.S. members starting later this quarter. America Online will integrate links to iTunes artists, albums and songs throughout its leading music site, AOL Music, which will give members the option to link directly to the specific iTunes Music Store page to preview and buy music as they browse and read music news and reviews.

And a Apple-Pepsi promotion will distribute free iTunes via soda pop caps next February:

Apple and Pepsi-Cola North America today announced a historic promotion to legally give away 100 million free songs to Mac and Windows PC users from Apple's iTunes Music Store. Beginning February 1, 100 million winning codes will be randomly seeded in 20 ounce and 1 liter bottles of Pepsi, Diet Pepsi and Sierra Mist, and the winning codes will be redeemable for a free song from the iTunes Music Store. Winners will simply go to Apple's iTunes Music Store (www.iTunes.com), enter the code found under the bottle cap and choose any 99 cent song from the online store's vast catalog of over 400,000 songs. The Pepsi iTunes promotion will kick-off with a Super Bowl ad on February 1, 2004, and will run until March 31, 2004.

Audiobooks from Audible Inc. are distributed exclusively through the iTunes Music Store:

Audible, Inc. and Apple today announced that more than 20,000 hours of audiobooks and other spoken word programs are now available for download exclusively from Apple's iTunes Music Store. Through iTunes, Mac and Windows customers can preview and download audio editions of

best-selling books, magazines, radio programs and original shows, manage audio content alongside their music collection, and take their entire audio library with them for listening anywhere with the market-leading iPod digital music player.

□ □ □ □ □ □ □ □ □ □ □ □

OPINION:

Technology vs. Legislation: iTunes for Windows and the RIAA

by Alan Graham

Mephistopheles :

Here to your service I will bind me;
Beck when you will, I will not pause or rest;
But in return when yonder you will find me,
Then likewise shall you be at my behest.
From Faust by Johann Wolfgang von Goethe

The buzz is that iTunes for Windows will be released on October 16th, and I'm dying to see how Apple handled DRM (Digital Rights Management) on the PC. What deal with the devil was negotiated in order to appease the RIAA (Recording Industry Association of America)? What compromises or balance did they have to strike?

It seems the only way to pacify the RIAA (MPAA{Motion Picture Association of America }, etc.) is to negotiate and compromise innovation. It is a sad state of affairs when we have to negotiate with a lobbying group as to what we can and cannot do with our technology. While the market has spoken, and the portable MP3 player is rapidly becoming the leading consumer electronic device, the RIAA has tried to bury technology for years.

1997 - Tries to kill off personal CD duplication.

1998 - Sued Diamond Multimedia over the Rio 300 MP3 Player, claiming it was in fact a recording device. This device was the bane of the music industry. According to the RIAA, combined with the Internet, it actually encouraged consumers to "infringe the rights of artists by trafficking in unlicensed music recordings on the Internet."

1999 - RIAA loses it's appeal in the case and says "We're obviously disappointed we lost in the Appeals Court. The court appears to have concluded that, despite Congressional intent, the Audio Home Recording Act has limited application in a world of convergent technologies. We filed this lawsuit because unchecked piracy on the Internet threatens the development of a legitimate marketplace for online music, a marketplace that consumers want. "

"Diamond declined our request to work together ... to adhere to the law," said Hilary Rosen, RIAA's president. "We believe [the Rio PMP300] is destined to damage the market for digitally downloaded music before it has a chance to begin."

Flash Forward to 2003

Four years later, Apple (fresh off the success of releasing the most popular MP3 player in history – the iPod) releases the iTunes Music Store. The first, truly comprehensive, yet simple execution of Digital Rights Management and online music sales. With over one million iPods and over 13 million songs sold, did the Rio MP3 player or the iPod destroy the market for digitally downloaded music, or did they in fact create it?

So given the apparent disconnect between the RIAA and the consumer, why is it we still consider

any compromise with them? They've had absolutely no vision when it comes to technology, and if it had been up to them, we would still be unable to burn music CD's, transfer music to MP3 players, or convert CD's to MP3's. In fact, if the mentality of the RIAA had been accepted years ago, there would not have been cassette tapes, reel to reel, or even CD's. If it had been up to the RIAA, our car stereos might have technical innovations like slot loading 45's.

The fact is the technology sector has always pushed the sales of media, when media sales began to decline. The CD injected new life into the music industry. The DVD increased sales in a video industry gone flat. Each time a new technology was proposed, however, large sections of the media industry fought tooth and nail to prevent it from ever seeing the light of day.

The RIAA argument is that technology encourages the average citizen to steal. The fact that I own a checkbook has not turned me into a bad check felon. The connection the RIAA tries to make between technology and piracy is absurd. Simply having a high speed internet connection and a MP3 player has not made me more prone to breaking the law.

The success of the iTunes Music Store is proof that if consumers are presented with a simple and affordable solution for purchasing music online, they will. And if the RIAA had worked effectively with the tech sector six years ago, we might have made more progress towards curbing piracy through solutions, not lawsuits against 12 year old girls.

We are on a slippery slope each time we make a concession with the RIAA. You can't work with a bully whose idea of working with you is telling you what to do and if you disagree, they'll take you to court. These tactics damage innovation because it sucks up valuable capital on lawsuits, driving small technology companies into oblivion. And let's face it, they are a large part of the reason why their wasn't an effective and acceptable DRM in the first place. If they spent more time talking and less time suing, the piracy problem might not be so rampant.

Do we need to protect artists, their work, and their livelihood? Of course, but that comes through empowering people, not rendering them powerless.

My major concern is what we may just compromise ourselves back to the phonograph.

If you have an opinion about this article, let me know about it - Dru

□ □ □ □ □ □ □ □ □ □ □ □ □ □

Thanks for taking the time to read this month's newsletter. Hope you enjoyed it. If you have any comments or suggestions for stories (or would even like to write a story - hint, hint, hint), please send them to me at machelpdesk@comcast.net Feel free to share this newsletter with a friend. The newsletter archives are located at <http://www.machelpdesk.com/page6a.html>. Y'all come back now, y'hear