



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 15, Number 4

April 2005

A Message from Dru

Well the news is in from Apple, and it's great! See Newsline for more info.



Happy Passover for those of our Jewish client/friends who celebrate this holiday of freedom from tyranny. For more info on Passover, go here - <http://www.jewfaq.org/holidaya.htm> or here - <http://www.holidays.net/passover/>.



For those of you who missed the recent e-mail about our rate increase -

Effective Monday April 4, 2005, due to the extraordinary high cost of fuel, we *temporarily* raised our rates as follows:

Hourly rates:

Individual - \$87.50 per hour [up from \$85/hour]

Corporate - \$97.50 per hour [up from \$95/hour]

Less-Than-Hour rates:

1 to 15 minutes - \$30 [down from \$50]

16 to 30 minutes - \$50 [remains the same]

Client/friends living further than 30 miles from Richardson, TX (as determined by MapQuest) will be billed at the rate of \$.36 per mile [down from \$.60 per mile] for the full round-trip mileage.

These rates will remain in effect until the price of gasoline drops below the \$1.75 per gallon level.



Thanks for your comments to all of you who saw me on the TV last month talking about my loading iPod business. If you'd like to see them (for the 1st time or) again, go here - <http://www.machelpdesk.com>. Then click on Files and Fun Stuff. Be aware that the files are 4.5MB and 4.8MB respectively (or about 14 minutes to download on a dial-up line). *And* if, by chance, you happen to have an iPod and want to save your the time in loading all those CDs, call me at the office and I'll happily do it for you. Prices start at \$1.29 per CD loaded.



Mac Security: Fact and Fiction

Most Mac users gaze on smugly as reports of each new Windows security crisis break. And they have good reason – research from anti-virus firm Sophos PLC showed that 68 viruses have affected the Mac since it was introduced in 1984 while 97,467 have affected Windows. Of those 68, most are a decade old or older and don't directly affect OS X.

However, although it may seem that there's no reason to worry about security on your Mac, you shouldn't think you're completely safe. Apple's regular Security Update releases prove that there is cause for concern, and common sense suggests that you're most vulnerable when you let your guard down.

So how can you tell the difference between scaremongering and true dangers? We examined seven common beliefs about Mac security - and show you what you really need to worry about.

Mac users don't need to worry about viruses. False

We've enjoyed a long, glorious stretch without serious malware affecting our platform. But that doesn't mean we can afford to let down our collective guard. 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.

If you can't name your antivirus program even though you're positive you've got one installed, you're half-way there. But this is a telltale sign that you haven't used it recently enough.

Just as important as having the software is making sure its virus definitions - the frequently updated information that antivirus software uses to recognize a virus - are up to date. The best way to do this is to check for definition updates regularly. If you use a product that has an automatic update feature, make sure it's turned on and set to a frequent update schedule.

Weekly updates should be adequate for most users, but if your computing involves accessing lots of files from lots of sources - whether via email, file servers, or Web downloads - then daily updates might be a better idea.

Be alert. Don't open unexpected email attachments until you've confirmed that they're from the sender they appear to be from. Research from Sophos shows that one in 18 emails circulating during November 2004 contained viruses.

Most malicious scripts affect only Windows machines, so if you click on one by accident, nothing will happen. But if you use Microsoft Word or Excel, you're vulnerable to some platform-agnostic macro viruses. Protect yourself by turning on the Warn Before Opening A File That Contains Macros option in each program (under program name: Preferences: Security), but be aware that not all macros are malicious. The person who sent you the document might have included a useful macro on purpose.

To further reduce the risk of infections, don't download free software or shareware from anywhere

but reputable sources such as VersionTracker.com, MacUpdate (www.macupdate.com), or the Apple software download page.

You're vulnerable to Windows viruses if you run emulation software. True

If you're running Microsoft's Virtual PC or another emulation product and running Windows, your Windows environment is susceptible to all the maladies that a stand-alone Windows PC is. Virtual PC and similar tools don't merely let you access Windows-created documents and run software intended for Windows machines; you're actually running the Windows operating system.

You can minimize the risk by keeping your Windows environment meticulously up-to-date via Windows Update, by turning on the built-in firewall in Windows XP's Security Center, or by installing your own firewall. That might mean running a Mac firewall and a Windows firewall.

It's also helpful to avoid some of the security holes that leave Windows users open to viruses and other malware. For starters, don't use Virtual PC's Virtual Switch network setting, which lets your virtual Windows computer act as though it were hooked directly to your network. If you put Windows right on your network with its own IP address, it's vulnerable to any network-based attacks, such as those that exploit Windows file-sharing vulnerabilities. Once Windows has been compromised, portions of your Mac's hard drive that have been shared within Virtual PC might be accessible.

Instead, use Virtual PC's shared-networking scheme (select Shared Networking in the Networking tab of each virtual PC's Settings dialog box). This offers protection similar to that of a company firewall or a home broadband router, separating your computer from the Internet at large.

Finally, if you're running Windows, you need antivirus software installed in Windows, not just on the Mac side.

Mac users don't need to worry about spyware. True

Breathe a long sigh of relief.

Spyware - programs that record information, such as browsing habits or keystrokes, and send it to a remote server - runs rampant on Windows, but there are currently no real spyware programs that affect the Mac. There are several programs that can monitor what you do by taking screenshots at different times and recording your keystrokes, but these programs are designed for people who want to monitor the activity of their Mac's users.

If you're a non-administrative user of a Mac on which an administrator has installed this type of program, there's not much you can do about it: you're not allowed to remove the software, since you don't have administrative rights. The best you can do is ask why it's there.

Sending chat messages is akin to throwing notes on loosely wadded paper across a crowded classroom. True

If you use any of the popular instant-messaging applications for OS X - iChat, AOL Instant Messenger (AIM), and MSN Messenger - someone watching your network traffic can read your messages easily. That sounds like the work of sophisticated computer hackers, but all it takes is access to your network (in your company, at home, or at a public Wi-Fi location, for example) and a packet-sniffing utility such as Brian Hill's MacSniffer.

Before you swear off instant messaging forever, ask yourself a few questions. Is it really likely that someone is scanning your network's data packets? You're probably safer chatting with a friend

from a single Mac at home than from a laptop connected to a free Wi-Fi network in a busy coffee shop. Does your conversation contain top-secret information? If most of your chats concern lunch take-out options, you probably needn't worry.

It's when you're discussing information that's private or proprietary that chatting can become the weak link your competition is waiting for.

When I'm using a wireless network at home, I'm totally safe. False

Wireless Wi-Fi networks use radio waves, which often extend well beyond the four walls of your home. That's no big deal if most of the inhabitants of your neighborhood are sparrows, but if you live in an apartment building or a dense urban area, it's easy for a neighbor or a visitor to a nearby business to hop onto the network. Less frequently, people might make it their mission to enter your network and try to access your computers.

Because you're not a Windows user, there's no current need to worry about people on your AirPort network corrupting your computer with viruses or malevolent programs. So far, there's no such animal that doesn't also require an administrative password. But you should be concerned if your network has no protection. In that case, someone could try to connect to your computers and browse your shared folders.

By default, guests can connect only to the Public folder in each user's Home directory, which means they can see only files that you've placed there on purpose. If you don't want uninvited guests to access that, secure your computers. Go to System Preferences: Sharing: Services, and turn off Personal File Sharing, Windows Sharing, Personal Web Sharing, and FTP Access.

If you don't want to risk anyone connecting to your computer, turn on wireless security. Under AirPort, you can enable WEP (Wired Equivalent Privacy). It's not the best security standard, but it will rebuff all but determined crackers. If you use AirPort Extreme and all of your computers are running Panther or Windows XP, you can opt for the stronger WPA (Wi-Fi Protected Access).

When I'm using a public hotspot, all of my passwords are being stolen. False

It's not technically true that your passwords for email, FTP, and Web sites are always being nabbed whenever you use Wi-Fi in a coffee shop, a hotel lobby, or an airport. But the potential is so high that you might as well consider it to be true.

People connecting to the same Wi-Fi network can see all the data passing over it if they have readily available free packet-sniffing software installed, and they can snatch your passwords, email messages, and files out of the air.

If you lug a laptop around for business or for pleasure, you can secure your Internet activities one by one. For instance, encrypt your email using a Web mail service that supports SSL (Secure Sockets Layer) for browsing or that can secure POP, IMAP, and SMTP with SSL. All major Mac email clients include SSL support.

In Apple's Mail, go to the Accounts pane in Preferences and select the Use SSL option in Account Information: Server Settings (outgoing email) and the Advanced tab (incoming email).

Web designers often need to transfer files to update Web sites while on the road. You can encrypt FTP using SFTP (Secure FTP). If you're running your own FTP server on OS X, turn on SSH (Secure Shell) on the machine that has the file repository. Go to System Preferences: Sharing: Services and turn on Remote Login and FTP Access. There is an increasingly large number of Web hosts that also support SFTP for transferring files. You need an SFTP-equipped FTP program

such as Interarchy, too, on the computer that's connected to your repository.

When you shop or bank online, your data is almost always already secured with SSL. But if you hate the idea of your surfing being observed, use a service such as Secure-Tunnel (www.secure-tunnel.com), which offers free anonymous surfing. Secure surfing costs \$8 per month.

If you want a more comprehensive way to protect your wireless activities when you're out and about, consider securing your sessions with a virtual private network (VPN) connection. A VPN encrypts all the data that enters and leaves a computer over a network connection, such as AirPort, preventing all snooping.

VPNs aren't just for corporations anymore. OS X Server 10.3 (Panther) includes both flavors of VPN servers currently in wide use. The regular version of Panther includes a VPN client. (Go to Applications: Internet Connect, and select File: New VPN Connection).

The Mac's default security settings are all you need to protect your computer from hacker attacks. False

Hackers attempt to attack your computer over the Internet by finding open, unsecured ports and exploiting them. A port is nothing more than a door through which computer data can be passed. Every computer has thousands of them, and every open port is a potential entry point.

Hackers attempt to find open ports by trawling the Net, sending out messages that your Mac understands as "anybody there?" When such messages hit your Mac (even if they hit a closed port), it behaves like a puppy dog, happily barking back, "Yep, I'm here!" That response lets hackers know there's something out there they can attempt to exploit. They'll then use port-scanning software to discover an open door they can get into.

To prevent this from happening, you need a firewall. A firewall is simply a piece of software or hardware that stands between your computer and the rest of the world, making sure that every piece of data coming or leaving through an open port on your Mac goes only where it's supposed to.

OS X has a firewall that's turned off by default. You can change that by going to System Preferences/Sharing/Firewall, and then clicking on the Start button. Frankly, there's no reason not to turn the firewall on if you always have your Mac connected to the Internet.

As soon as you start the firewall, all the ports on your Mac are stealthed.



NEWSLINE

Apple to Ship Mac OS X "Tiger" on April 29

More Than 200 New Features & Innovations

Apple announced that Mac OS X version 10.4 "Tiger" will go on sale Friday, April 29, beginning at 6:00 p.m. during special events at Apple's retail stores and Apple Authorized Resellers. Tiger has more than 200 new features and innovations including Spotlight™, a revolutionary desktop search technology that lets users instantly find anything stored on their Mac, including documents, emails, contacts and images; and Dashboard, a new way to instantly access important information like weather forecasts and stock quotes, using a dazzling new class of applications called widgets.

“Mac OS X Tiger is the most innovative and secure desktop operating system ever created,” said Steve Jobs, Apple’s CEO. “Tiger’s groundbreaking new features like Spotlight and Dashboard will change the way people use their computers, and drive our competitors nuts trying to copy them.”

Spotlight is Apple’s new lightning fast way for users to find virtually anything stored on their Mac. Much like users can instantly find songs in iTunes by name, artist or album, Spotlight searches the contents inside documents and information about those documents, or metadata, to find just about anything - emails, contacts, appointments, images, PDFs, and almost any type of document, including Microsoft Office documents - then automatically organizes and instantly displays the results. Because Spotlight technology is built right into the core of the operating system, it automatically updates results instantly whenever files change and enables developers to incorporate Spotlight technology into their applications. Apple has incorporated Spotlight search technology into several Tiger applications including Mail, Address Book, Finder and System Preferences, and several third party developers are expected to introduce applications with Spotlight search technology in the coming months.

Dashboard is a new world of beautiful accessory applications called widgets that appear instantly to give users immediate access to information like stock quotes, weather forecasts, airline flight tracking, unit of measure, currency conversions and a phone book. With a single click a user’s favorite Dashboard widgets instantly appear with up to the second information; with another click they’re instantly gone and the user is right back to where they left off. Tiger ships with 14 widgets, and because Dashboard is based on standard web technologies such as HTML and JavaScript, it’s easy for third party developers to create new widgets that users can easily add to their Dashboards.

iChat in Tiger supports the stunning new H.264 video codec for dramatically better picture quality over the same Internet bandwidth. Users can now create audio conferences with up to 10 people and video conferences with up to four people in a 3D virtual conference room, just as if they were all seated together at a table*. In addition, contacts on a Buddy List can now see which iTunes song a user is playing and view it in the iTunes Music Store with just one click.

The new Automator workflow application lets users easily automate repetitive tasks without complex programming. Users simply select from a library of more than a hundred customizable actions and drag and drop them to create an automated workflow, specifically tailored to suit their requirements. Once created, workflows can be saved and even shared with friends and colleagues.

A full featured RSS reader is built into Safari™ to provide instant access to the most current information from leading news organizations, community web sites and even personal weblogs (blogs) directly from the browser. Multiple RSS feeds can be merged into one easy-to-read interface to create a user’s own personal news clipping service.

Other new features in Tiger include:

- QuickTime 7, the latest version of Apple’s standards-based media player, with H.264 support, live video resizing, zero-configuration streaming and extensive surround sound;
- Mail 2, a dramatically enhanced new version of the Mac OS X built-in Mail application with a new user interface, Spotlight searching, .Mac syncing and full screen slideshow;
- iCal 2, with support for birthday calendars, calendar groups, improved printing and Spotlight and Automator functions;
- Font Book 2, the updated font management utility included in Mac OS X that now supports libraries for installing fonts anywhere on the system or network; and
- a completely new .Mac sync preference using Xsync, a new sync engine built into Mac OS X that enables .Mac subscribers to automatically synchronize their Safari bookmarks, iCal appointments, Address Book contacts, Keychain passwords and Mail settings across multiple computers.

New core technologies and tools in Tiger make it easy for developers to create the next generation of innovative applications, including:

- native 64-bit application support to take advantage of the increased performance unleashed when accessing massive amounts of memory, while still running side-by-side with existing 32-bit applications;
- Core Image and Core Video to provide the foundation for new image and video processing applications;
- Xgrid™, Apple's easy-to-use distributed computing software;
- improved Windows compatibility to make it even easier for Mac OS X users to access a Windows-based home directory and authenticate against Microsoft's Active Directory;
- major advances to the open standards UNIX-based foundation including an updated state-of-the-art kernel with improved SMP scalability, 64-bit virtual memory, Access Control Lists, GCC 4.0 and modernized network services; and
- Xcode™ 2, the latest version of Apple's powerful suite of developer tools, designed to make it even easier and faster to build innovative Mac OS X applications.

Pricing & Availability

Mac OS X version 10.4 "Tiger" will be available on April 29 beginning at 6:00 p.m. at Apple's retail stores and through Apple Authorized Resellers for a suggested retail price of \$129 (US) for a single user license. Visitors to the Apple Store (www.apple.com) can pre-order copies of Tiger beginning today. The Mac OS X Tiger Family Pack is a single-residence, five-user license that will be available for a suggested retail price of \$199 (US). Volume and maintenance pricing is available from Apple. The standard Mac OS Up-To-Date upgrade package is available to all customers who purchase a qualifying new Mac system from Apple or an Apple Authorized Reseller on or after April 12 for a shipping and handling fee of \$9.95 (US). Tiger requires a minimum of 256MB of memory and is designed to run on any Macintosh computer with a PowerPC G5, G4, or G3 processor and built-in FireWire.

* Initiating a multiway video conference requires a PowerPC G5 processor or dual 1GHz G4 processors and 384 Kbps or faster broadband Internet access. Participating in a multiway video conference requires a 1Ghz G4 or dual 800 MHz G4 processors or faster and 100 Kbps broadband Internet access.



Apple Sings a Happy Tune; \$290 Million Q2 Profit on iPod Growth

It was another successful quarter for **Apple Computer**, as the Mac and iPod maker exceeded estimates posting a net fiscal second-quarter profit of US\$290 million, or 34 cents a share - 10 cents better than the street estimate.

Revenue for the quarter was \$3.24 billion, up 70% from the year-ago period of \$1.91 billion. Gross margin was 29.8%, up from 27.8% in the year-ago quarter. International sales accounted for 40% of the quarter's revenue, the company said.

Analysts surveyed by Thomson First Call had forecast Apple to earn 24 cents a share on \$3.21 billion in revenue. Apple predicted in January that it would earn 20 cents a share in the just-completed quarter, on \$2.9 billion in sales.

During the same period a year ago, Apple earned \$46 million, or 6 cents a share on \$1.9 billion in revenue. The Q2 profit rose more than sixfold compared to a year ago.

As early as Wednesday afternoon, analyst Keith Bachman of Banc of America Securities **warned**

