December 2008
Double Click
Main Meeting Report

*(**If any Double Click member is interested in helping out with the newsletter, please contact one of the Double Click officers.**)*

Our December meeting included a Beginners presentation, a Q&A session, the main presentation and ended with our monthly prize raffle. Attendance was a bit higher than average.

Beginners Session - December

A Few Simple Mac Tips

Here are a few simple tips I use when using my Mac that I would like to share with you.

Drag to the Desktop

Clippings. In most applications available for Mac OS X today (those that are based on Apple's Cocoa programming language), you can select text and then drag that text to the desktop to create a Clipping File. To do this, first use the mouse cursor to highlight some text. Then release the mouse button. Next, click and hold the cursor anywhere in the text that you just highlighted. (Note: If you click and then release the mouse button, your original selection will no longer be selected, and you'll have to start over again.) Finally, with the mouse button still held down, drag the highlighted text onto the desktop. When you release the mouse button, a text clipping will be created on the desktop. If you double-click on the text clipping icon, a small window will open to display the copied text as shown below.

You can copy and paste this text into a document. However, this is an "all or nothing" proposition. It's not possible to highlight a portion of the text clipping to copy and paste. Only the full contents of the clipping may be used. Thus, you don't have to highlight anything in the clipping. Just select Copy from the Finder's Edit menu (or the keyboard shortcut, Command-C, ⌘-C) and then paste the clipping's contents into your document.
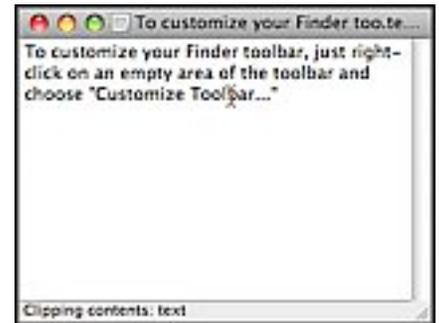
Clippings aren't limited to text. Often, you can select a graphic (say, from a web page) and make a clipping out of it. The same technique applies: drag across the graphic, then click and hold on the graphic, and finally drag to the desktop.

URLs. If you don't want to save a web page in your web browser's bookmarks list, you can still save a link to the web page. The simplest way is to click and drag the small icon that appears just before the web page URL in

your browser. If the icon isn't present, you can still highlight the text in the URL and then click/hold/drag the text to the desktop. A web location file (.webloc) will be created on the desktop in manner similar to creating a clipping file. This works (at least in Apple's Safari web browser) for URLs imbedded in a web page. Again, just select/release/click/hold/drag the URL to the desktop.

Application Switcher
If you have a number of applications open, you may find it convenient to switch among them by using the Command-Tab (⌘-Tab) keyboard shortcut. This brings up the Application Switcher built into Mac OS X. Use ⌘-Tab to bring up a display of open applications. Then while continuing to hold down the Command key, use the tab key to move forward through the list of open applications. Add the Shift key to the sequence (Shift-⌘-Tab) to move back through the list while it's displayed.

Want to quit an application while in the Application Switcher? Simply tab to the desired application, and hit the Q (for quit) key.

New in Mac OS X, 10.5 (Leopard) is the ability to drag a file onto an icon in the displayed list of applications in order to open it in an application other than the one that it's normally opened from. Click on a file located on the desktop, drag it, use ⌘-Tab to open the Application Switcher, and drag the file onto the desired application to open it.

Window Switching
Use ⌘-~ to switch through the open windows in a given application.

> Note: ~ is the tilde symbol. It's found on a key at the upper left of the keyboard, often just below the Escape or esc key, along with the Grave Accent (`) symbol.

In the Finder, window switching also includes the desktop. As with the Application Switcher, add the Shift key (Shift-⌘-~) to move back through the list of open windows while the list is displayed.

Zooming the Display
On LCD displays, the prominent type available today, sometimes what is being displayed is just a little too small to read comfortably. Fortunately, Apple

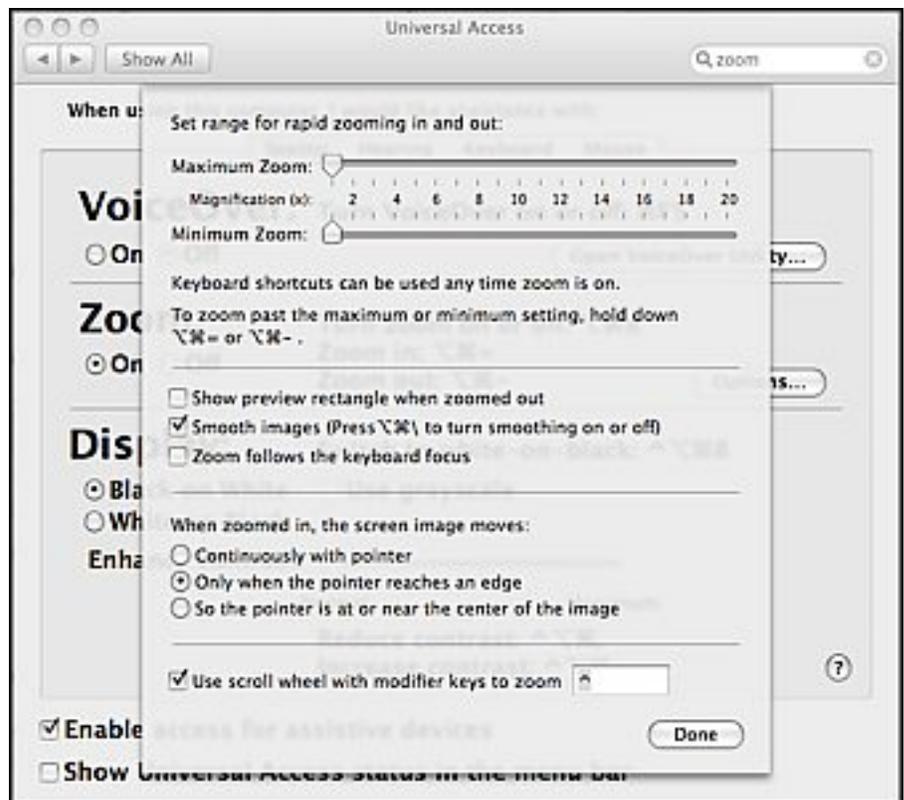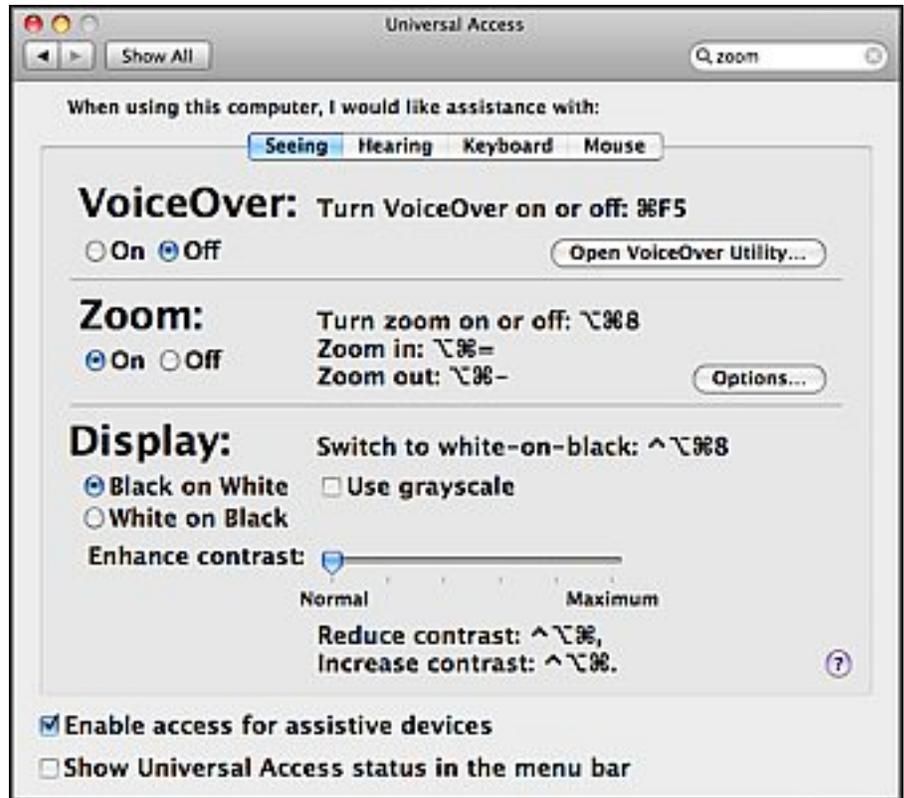has provided a means to zoom into a particular area and make it display larger.

First open System Preferences (by selecting it from the Apple Menu). Then, click the "Universal Access" icon. The resulting window that is displayed is shown to the right.

In the Seeing tab, look at the Zoom section. Here you can turn the Zoom function on and off. Also, the default keyboard shortcuts are listed for turning zoom on or off, zooming in, and zooming out.

Clicking the Options… button provides you with some additional zooming capability.

In the resulting Options window, you can set the maximum and minimum amounts for zooming (as controlled by the keyboard shortcuts).

There are several other zoom settings that can be adjusted. The one that I've set and use most frequently is the setting for using the scroll wheel on your mouse along with a

modifier key to scroll continuously. (See the bottom section of the window.) Click on the checkbox to use the scroll wheel on your mouse for zooming. Also, press the modifier key that you wish to use. The default is the Control key (^ symbol). You can also use the Command (⌘), Option (⌥), and Shift (⇧) keys or any combination of them if you wish.

The Dictionary

Another valuable feature offered by Mac OS X is its dictionary capabilities. A full-featured dictionary is available based on the New Oxford American Dictionary. In addition to being able to look up words in this dictionary, the dictionary function also allows words to be looked up in Wikipedia, the Oxford American Writer's Thesaurus, and Apple's own dictionary.

The Dictionary is a separate application (found in the Applications folder). It can be used as a standalone application, or it can be invoked as you review documents and want to look up a word. In the documents for most applications, simply place the cursor in the word you wish to look up (or click on the word or double-click on the word to select it if you wish) and then use the keyboard shortcut, Control-⌘-D (^-⌘-D). (This is the default keyboard shortcut,

but you can change it if you wish through the Keyboard Shortcuts tab in the Keyboard & Mouse system preference.) A small window opens up next to the word providing a brief explanation.

If you want a more thorough explanation, just click on the More… button at the bottom right corner of the window to bring up the comprehensive explanation from full dictionary application.

If you want to skip to the comprehensive explanation right away, simply right-click (Control-Click, ^-Click, if you don't use a two-button mouse) to bring up a contextual menu. "Look Up in Dictionary" should be one of the selections.

January 18 Beginners SIG Meeting

At the January Beginners SIG meeting, we'll explore another Mac topic.

--Steve Parker

"Q & A" Sessions / Announcements

The December Questions and Answers session (as usual) covered a wide range of topics.

Note: We would like to expand the meeting report coverage of his discussion and need someone to help take notes of the questions and answers during this session at our monthly meeting. If any member can do this for us on a regular or semi-regular basis, *please volunteer!*

Member Presentation

Double Click members have an opportunity to address their fellow members at a main meeting.

The **"3 Minute Ticker"** is an opportunity for you to tell the rest of us at the meeting about a great computer program or feature you came upon... or something that turned out to be a waste of money! You could tell us about your best (or your worst) computer purchase, hardware or software, or perhaps about a good or bad experience relative to computer service. Share it with the rest of us! As the title of this feature implies, members will have three minutes to tell their story. A limited number of speakers (one or two) will be featured each month.

"Tell Us About Your Business" provides Double Click members an opportunity to introduce the group to their business in a five to 10 minute talk. Suggested points that you may wish to address would be:

• are you the owner, or a key employee?
• when did your business start?
• what product or service does your company provide?
• tell us about the Mac computers you use.
• how can Double Click members help you?
• what do you consider a good referral?

Your membership in Double Click provides you access to computer expertise... now it may also improve your customer base. There may be customers for you right in the room!

Members interested in presenting a "3 Minute Ticker" or "Tell Us About Your Business" talk should email the member talk coordinator, Jerry Smaglik, at <jsmaglik@wildblue.net>.

Main Presentation

"Macintosh Security: Local and Net-wide"

Presented by Kevin Sears and Jim Macak, Double Click officers

Internet Security

Kevin Sears started the presentation using a Keynote slideshow, discussing malware and phishing.

Malware

Definitions
Malware is a term used to identify <u>Ma</u>licious Sof<u>ware</u>. Malware is written for a variety of purposes, ranging from bragging rights to profit motives. Types of malware include viruses, worms, trojan horses and rootkits.

The term virus is often used as a "catch-all" phrase. A virus is able to copy itself and infect a computer without the knowledge or permission of the user. The majority of viruses also contain a payload of malicious code that cause damage by deleting or corrupting files.

Worms propagate themselves, rather than using a carrier program or file. Worms create exact copies of themselves and use communication between computers to spread. Internet worms can travel between connected computers by exploiting security "holes" in the operating system.

Trojan horses are programs that pretend to be legitimate software, but actually carry out hidden, harmful functions. Many Trojan horses install software that allow an attacker remotely control or monitor your computer.

A rootkit consists of a program (or combination of several programs) designed to take fundamental control of a computer operating system by gaining administrator(or "root") privileges. Techniques used to accomplish this

can include concealing running processes from monitoring programs, or hiding files or system data from the operating system.

Malware Propagation
E-mail is the most effective vehicle to deliver malware, usually as an attachment. E-mail is a low cost transport method with access to wide distribution lists. Once the attachment is opened, the malware program can go to work.

Preventive Measures Against Malware
• Keep your Operating System up to date with the most recent patches.
• Make sure your computer has a firewall and anti-virus software. You must keep the definition files up to date to ensure protection.
• Avoid downloading unknown software or software from a non-reputable website.

Phishing

Phishing is an attempt to fraudulently acquire sensitive information such as usernames, passwords, SSN's, and intellectual property by masquerading as a trustworthy entity. Typically phishing occurs in an email, but also accomplished via telephone or other electronic means.

Initial phishing attacks were amateurish campaigns that used email and websites laced with poor grammar and graphics in an attempt to gather personal data. Today's sophisticated attacks target business users and executives with the intent to install malicious programs that steal intellectual property and cause harm to the enterprise.

Be wary of:
• Emails from unknown senders
• Unexpected or unsolicited information
• Urgent requests for information or action
• Links or attachments in unsolicited or suspicious emails
• Contextually relevant emails from unknown senders
• Requests to upload or download data

How to handle possible phishing
• Do not click on links or attachments in suspicious emails.
• Only open attachments you expect to receive from known senders.
• If you receive an email from a known sender that appears suspicious, phone the sender to validate the message.
• When in doubt, report suspicious email. Create a new message and attach the suspicious email. This preserves the e-mail header information which is needed for investigating.

Phishing Resources

• Anti-Phishing Working Group
The Anti-Phishing Working Group (APWG) is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types.
http://www.apwg.org/

• PhishTank
PhishTank is a collaborative clearing house for data and information about phishing on the Internet.
http://www.phishtank.com

• MillerSmiles
An internet's anti-phishing site, maintaining an archive of phishing and identity theft email scams. Also runs a news service which provides the latest headlines from the world of fraudulent emails and phishing.
http://www.millersmiles.co.uk

• SpamFo
The site is a central resource of all information relating to spam, with topical news, reviews, FAQs and useful links.
http://www.spamfo.co.uk/

Other Resources

• ClamXav
A free anti-virus checker for Mac OS X
http://www.clamxav.com/

• Security Software reviews (Windows only)
http://www.2009securitysoftwarereviews.com/

• MacScan
Anti-spyware security software for Macintosh OS X
http://macscan.securemac.com/

• SANS @Risk: The Consensus Security Alert
Weekly report that summarizes the three to eight computer vulnerabilities
that matter most, tells what damage they do and how to protect yourself
from them
- http://www.sans.org/newsletters/risk/

• Talisker Computer Network Defense Operation Picture
A website that actively tracks current internet-wide security status
http://www.securitywizardry.com/radar.htm

Jim Macak continued the Security presentation, discussing options available
on OS X - Leopard to help secure or "harden" one Mac.

Better Safe than Sorry...

Our Macintosh computers have historically been much less prone to com-
puter "malware" (viruses, trojans, worms and other security compromises)
than other personal computers. With the arrival of OS X, this relative safety
has not only continued but has improved. OS X is inherently a more secure
operating system than OS 9 and earlier. Apple proactively addresses secu-
rity issues with "Security Updates" and security fixes are always present in
major Mac OS X System updates.

Consequently, many Macintosh users have become somewhat complacent
with respect to security issues on their Macs. However, some would argue
that it is time for us to become more concerned…

Potential security vulnerabilities of OS X and applications that run under OS
X continue to be discovered as time goes on. Although these vulnerabilities
have not resulted in "real world" problems, the potential exists for problems

to arise. Many of these vulnerabilities have been fixed via software updates and others can be obviated by implementing some basic security practices. However the existence of these potential security vulnerabilities should serve to remind us that Mac OS X is not immune to malware attacks and other security issues.

What should you do to protect your Macintosh from security threats?

The "knee-jerk" reaction would be to install some brand of OS X anti-virus/security program. This was certainly good advice for Mac OS 9 and earlier, but it's questionable if these programs are currently necessary or desirable for Mac OS X. Several anti-viral programs have been implicated in causing occasional problems and undesirable side-effects. Given the fact that, as of this writing, we have yet to see a real world malware threat to Mac OS X, perhaps anti-virus utilities are "overkill."

A possible exception to this generalization about installing anti-viral software would be a user who regularly works with documents generated by Microsoft programs running on Windows computers, as such documents may contain "macro" viruses. Although a macro virus will not directly attack Mac OS X, it can be an annoyance and can be passed on to other users. An anti-virus utility running on your Mac would detect macro viruses. Thus, if your Mac use fits this scenario, you may wish to consider installing an anti-virus utility.

What else might we do to secure our Macs?

Following are some basic suggestions for improving the security of an OS X Macintosh that you should definitely consider implementing on your own system.

• **Install Security Updates.** As noted above, Apple issues security "fixes" when a solution for a potential problem becomes available. Don't delay more than a day or two before installing these software updates. Also, be sure to perform timely updates of third-party software.

• **Keep anti-viral software updated.** If you decide to use an anti-viral utility, it is imperative that you update it regularly. Your software won't find

the latest malware if its virus scanner is out-of-date. You should check for updates on at least a weekly basis.

• **Backup critical data.** Not only will the ramifications of a catastrophic security breach on your Macintosh be minimized by a regular backup routine, but the untoward effects of user errors, software bugs and hardware malfunctions will be decreased too. The need for regular backups is crucial.

• **Implement a hardware or a software firewall.** If your Mac is on a network or Internet-connected, your system is at risk to external attack. Firewalls decrease this risk by not allowing certain (or all) external connections to your computer. Most routers (that connect between your cable or DSL modem and your Mac) provide a hardware firewall. Mac OS X includes a free software firewall, which you can enable from within the "Sharing" pane of System Preferences.

• **Use a "Standard" account.** The "Admin" account that was set up when you first installed OS X allows many activities that a Standard account disallows. A malware program run under the Admin account may more easily create problems on your Mac than when run under a Standard account. Hence, using your Mac on a day-to-day basis under a Standard account may be safer.
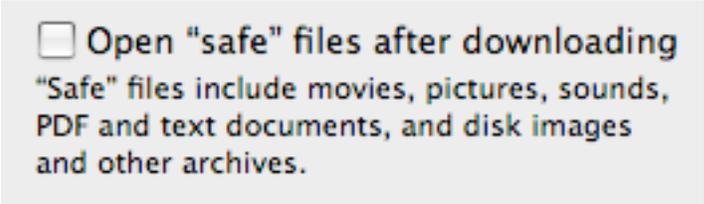
• **Be wary of email.** Attachments and html-formatted messages are one vector for malware to enter your computer. Don't run email attachments or click in the body of html-formatted messages that you have received from a sender of uncertain integrity. (This is especially important if you read email under an Admin account.)

• **Encrypt sensitive data.** Files on your Mac that contain sensitive and private information can be encrypted to safeguard them from prying eyes. The built-in "FileVault" capability of OS X will encrypt your complete Home folder such that only you or the computer's Administrator can read the files. Furthermore, even if you do not use "FileVault," you should enable the "Use secure virtual memory" option in the "Security" pane of System Preferences.

• **Use "strong" passwords.** OS X uses passwords to enable access to user accounts, allow software installation, decrypt files, etc. A strong password is one that cannot be easily guessed by an outside agent. The word "password" is not a good password, nor is "123" nor is your first name! Strong passwords are lengthy and include numbers and punctuation and cannot be easily guessed by someone else.

• **Be wary of file downloads.** It is strongly recommended that you turn *off* the option to "Open 'safe' files after downloading" in Safari's General preferences. Use the Finder's "Get Info" function to check downloaded files to be certain they really are what they are purported to be before you run or open the download. Remember, downloading a malicious file is akin to inviting a robber into your home. Only download files from "trusted" sources.

These suggestions cover some of the basics of Macintosh security. They are not all-inclusive, however. The more "connected" your Mac is to other computers and networks and the more accessible your Mac is to other people, the stronger your security precautions should be.

Macintosh Security On-Line Resources

• Leopard Security Configuration
A comprehensive guide from Apple that provides instructions and recommendations for securing Mac OS X version 10.5 or later, and for maintaining a secure computer.
[Mac OS X Security Configuration for Version 10.5 Leopard](#)

• Corsaire Technical White Paper
A guide by an internet security company.
[Securing Mac OS X Leopard (10.5)](#)

• NSA Security Configuration Guide
Your government's guide to "hardening" OS X
[Mac OS X Hardening Tips](#)

double Click

January 18th Meeting Preview:

"Windows on Your Mac:
Quick Switching Between
Windows and OS X - Leopard"

Presented by
Peter Lee, Double Click member.

Peter will discuss how to use "virtual machine software" such as Parallels and VMWare Fusion to run alternate operating systems on your Mac.

Check the Double Click website for more meeting information:

www.double-click.org

Made on a Mac.