

The ACCC Public Labs

CONTENTS

The ACCC
Public Labs

1

ACCC Lab
Locations

2

Safe Email
Viewing

3

Eudora Options
for Safe Viewing

5

Safe Email
Viewing in
Outlook

6

Flu Shots for
Your Computer

7

Head Crash:
Securing Email &
Editing PDFs

11

The Campus Beat



Who Can Use Them

Use of the ACCC computer labs is free and available to all UIC students, faculty, and staff who have a current valid phonebook entry. If you already have a UIC email account, chances are you also have an account for logging in to the lab computers. Just use your netid and ACCC common password to log in. If you do not yet have a lab account you can easily create one at a Windows XP machine in one of the labs by following instructions posted next to the monitor. Your lab account will be available for use within minutes.

Information about the Labs

Information about the ACCC public computer labs is available on the ACCC Web site at <http://www.accc.uic.edu/>. Click the purple **Facilities** button. The pages describing the labs are in the section at the top, "Public Computer Labs."

Click **Public Labs - Hours and Locations** for a list of labs; click on the lab name to see detailed specs on machines for the lab. Most labs have Pentium III or IV machines running Windows XP. Mac G4 and G3 machines are also available in some labs; most are currently running OS X and the rest are being converted. Zip drives and CD-ROM drives are standard, and some labs have machines with CD-RW and DVD drives. There are labs on both sides of campus that are always open. (See page 3.)

Many of the labs can be reserved for classes that would benefit from hands-on instruction.

Printing in the Labs

Lab users are allotted \$15 worth of free printing each academic term through the U-Print system. If you use all of your free pages, you may continue to print for a per-page fee by putting money on your

i-card or add to or purchase a UIC Flames card at a Card-add Value Station (CVS). Card-add Value Stations are located in or near most computer labs.

You can check your print quota and usage online by selecting the link **Printing - the U-Print System** on the Facilities Web page. Print quotas are reset one week before each new term and do not carry over; however, monetary value on a card does.

Another nice feature of the U-Print system is that you may select any printer on the system to retrieve your output, and you have up to 12 hours to do so. You are not charged for the print job until you log in to a Pharos station and print it.

Lab Software

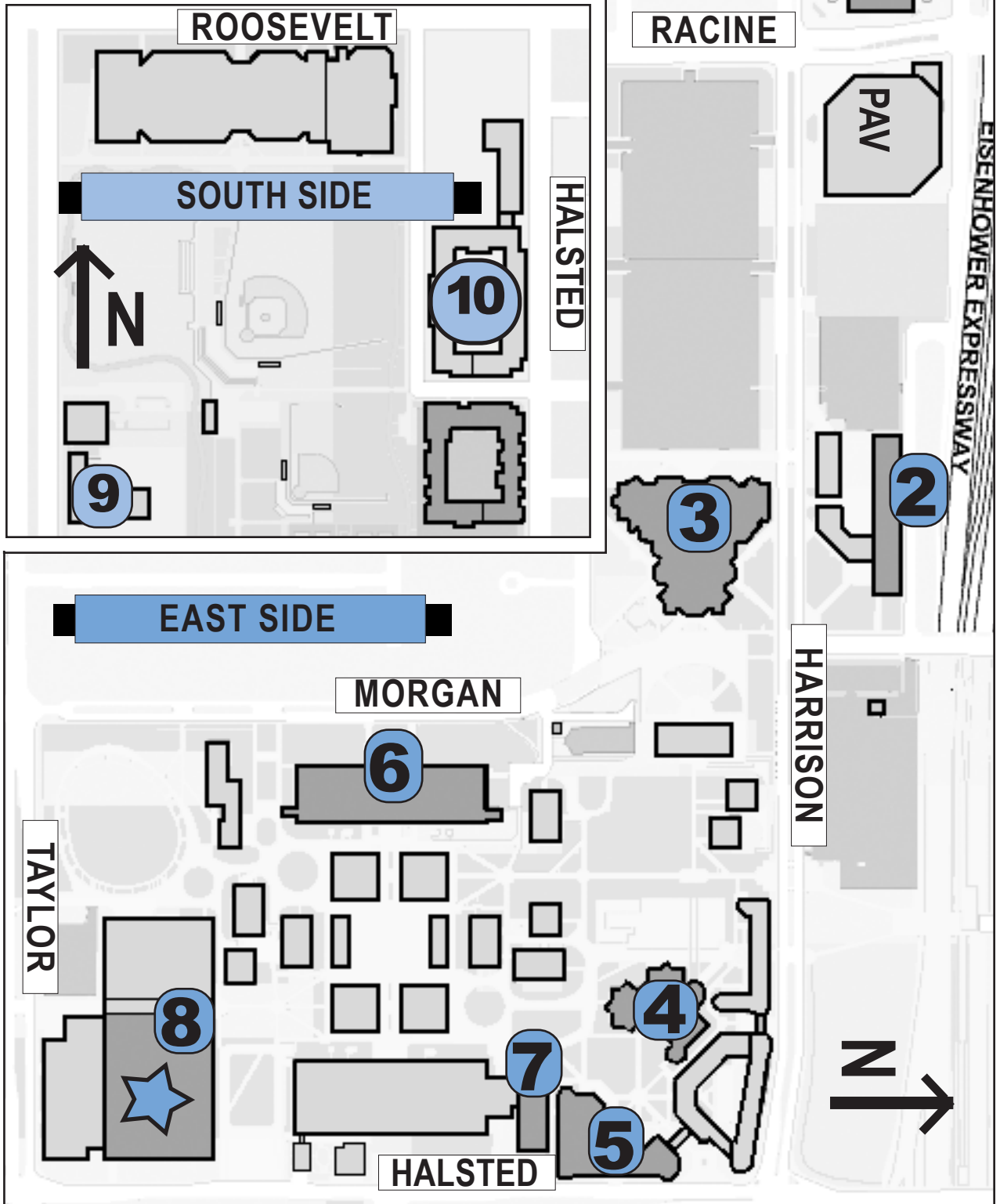
Software available in the labs ranges from general-purpose applications, such as word processors and Web browsers, to specialized applications installed for specific classes. Click **Public Labs - Software** on the Facilities page for a complete list of installed applications. Instructors can request that additional software be installed — the ACCC will do the installation, provided that the application can be made to work in the lab environment. The request must be made four weeks in advance and must be accompanied by proof of licensing. Instructions and forms for requesting software installation as well as for reserving labs are also on the Facilities page.

Keeping the Labs Clean

The ACCC works hard to keep the labs in good shape for the UIC community. Lab machines are serviced as needed and are cleaned thoroughly during break periods. Your cooperation is essential for keeping the labs clean and usable for all. And, as always, protect your account by making sure you log out before you leave the lab.

ACCC Lab Locations

No food or drink, open or closed, is allowed in any ACCC lab, ever. People violating ACCC lab rules are subject to account suspension.
<http://www.accc.uic.edu/policies/pcpolicy.html>



LEGEND

- a** accessible
- i** can be reserved for classes
- c** ACCC consulting available
- b** building access required after hours; fill out a form at CSO, 2267 SEL, or 181 or LL55 BGRC. Allow 1-2 weeks for processing.

Student Services Building

1200 West Harrison Street
2300 SSB
M-F: 8:30 a.m.-6:00 p.m.

1

a, c

Education, Performing Arts, and Social Work

1040 West Harrison Street, L270 EPASW
M-W: 9:00 a.m.-9:00 p.m.,
Th: 8:00 a.m.-9:00 p.m., F: 9:00 a.m.-6:00 p.m.,
Sa and Su: 1:00-5:00 p.m.

2

a, i

Behavioral Sciences Building

1007 West Harrison Street
B001 BSB
M-F: 9:00 a.m.-9:00 p.m.

3

a, c

Art and Architecture

845 West Harrison Street
2312 AA
M-Th: 9:00 a.m.-7:30 p.m., F: 9:00 a.m.-6:00 p.m.
B120 AA
M-Th: 9:00 a.m.-9:00 p.m.,
F: 9:00 a.m.-5:00 p.m., Su: 1:00-9:00 p.m.

4

a, i

Student Residence and Commons

700 South Halsted Street
2027 SRC
M-F: 9:00 a.m.-9:00 p.m.

5

a, c

Richard J. Daley Library

801 South Morgan Street
1444 LIB
open during library hours

6

c

Chicago Circle Center

710 South Halsted Street
401 and 408 CCC
M-F: 9:00 a.m.-9:00 p.m.

7

a, i, c

Science and Engineering Labs

950 South Halsted Street
2054*, 2058*, 2249, 2249F, 2263, 2265 SEL
24 hours
(*M-F: 9:00 a.m.-9:00 p.m.)

8

a, i, c, b

School of Public Health and Psychiatric Institute

1601 West Taylor Street, B34 SPHPI
M-F: 7:15 a.m.-7:00 p.m.

13

a, i

Benjamin Goldberg Research Center

1940 West Taylor Street
179 and 105 BGRC
M-F: 9:00 a.m.-5:00 p.m.

12

a, i, c, b

24 hours with building access (see Legend)

Labs For Building Residents Only

Marie Robinson Hall
811 West Maxwell Street
158 MRH; 24 hours

9

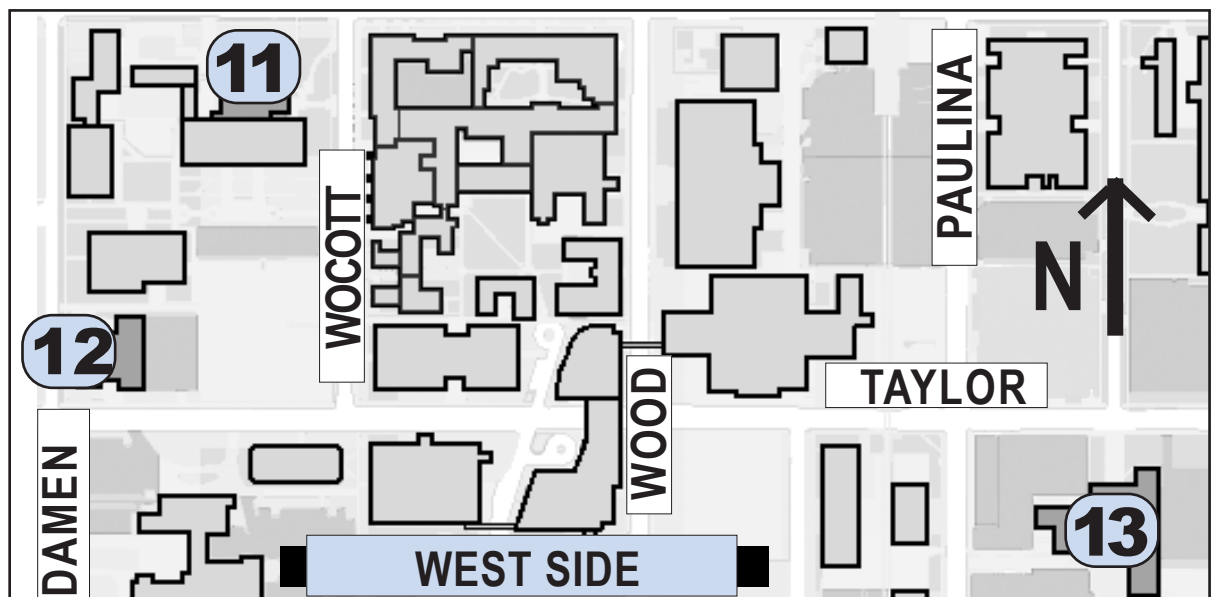
Thomas Beckham Hall
1250 South Halsted Street
181 and 183 TBH; 24 hours

10

Student Residence Hall
818 South Wolcott Avenue
317 SRH; 24 hours

11

All Resident Hall labs are accessible.



Safe Email Viewing

System Icons:



The Internet and
the World Wide Web



Apple Macintosh



MS Windows



Linux

Readership Icons:



Everyone



Novice



Expert

Tech Tips



When you take a cake out of the oven, you use a pot holder; when you drive, you put on your seat belt; and you even get a flu shot every year. But are you that careful when you read your email? Here are the three basic principles of safe email viewing, along with the essential principle for being safe when you're connected to the Internet.

Principle Number 0, The Basic Requirement for Safe Computing at UIC: Download and install Norton/Symantec Antivirus and run LiveUpdate on a regular basis.

Norton Antivirus is owned by Symantec and has been renamed Symantec Antivirus. By one name or the other, it's free to the entire UIC community. You can put it on all of your computers, and it works. It even finds viruses and worms that have been renamed to .txt files on the server by Mimedefang. Once you get NAV/SAV going, your only vulnerability is the first day or two after a virus is released, until Symantec develops and releases a definition file including the new virus, and then until you download and install the definition file.

Principle Number 1: Before you open any email message, check its subject and whether it has an attachment, and never open any email message you're uneasy about.

I'm sure this sounds sensible, but most email programs make it very difficult to accomplish. There are two ways that they conspire against you:

- preview panes
- automatically opening email

Both Eudora and Outlook come with a "preview pane" turned on by default. It helpfully opens the first — and next — email message for you, whether you want to see it or not.

In Eudora, the primary problem is that the preview pane can be

unstable and cause Eudora to crash, and there is the further problem that the default viewer for the preview pane is an embedded Microsoft Internet Explorer, which can also be exploited.

In Outlook, previewing messages is downright dangerous. I don't know whether it's because Outlook is that much worse than any other email program or if it's just because it is so widely used that an Outlook worm can have a major effect. Either way, Outlook is the primary target of email viruses and worms, and just opening a message in Outlook can be enough to set them loose.

Most email programs allow you to go directly from viewing one email message to viewing the next. That's not quite as dangerous as using a preview function, particularly if you've gone through the mailbox's index and deleted all the spam and suspicious email before you start reading the rest of your email. But new email can come in that you haven't checked out and you could get burned.

Principle Number 2: Don't download and/or use attachments unless you've double-checked that they're legitimate.

Yes, yes, I know, you're tired of hearing everyone saying this, but one major email virus or worm after another proves that people aren't listening.

There are two parts to this.

(1) Prepare your computer:

You run Norton or Symantec Antivirus, so you don't have to worry, right?

Well, sort of.

You are prepared if you have NAV/SAV's LiveUpdate scheduled to run automatically, on a regular basis, say once a week, at a time when your computer is turned on and connected to the Internet. If your computer is not connected to the Internet on a regular schedule, set an alarm to remind you to run it yourself once a week. (Wednesday afternoon or later is a good time; that's when Symantec releases regular updates.)

Even if you do run LiveUpdate regularly, you're not safe just after a new email virus or worm gets loose. Whenever you hear about a new one, it's a good

AntiVirus for Email

If you run the automatic antivirus protection of Symantec AntiVirus for Windows (Realtime File Protection) and Norton AntiVirus for Macs (Auto-Protect) all the time, it will protect you from viruses in your email as you download and read it. Make sure you turn these features on when you install SAV or NAV. See "Flu Shots for Your Computer," on page 7. (In Mac OS 8.1 through 9.x, NAV doesn't support all email clients, but it does support Eudora and Outlook. In OS X, it supports all email clients.)

About Outlook

The ACCC doesn't support or recommend using Outlook or Outlook Express for email. That means we don't have much experience with it. If you have questions about Outlook, we'll answer them if we know the answer.

idea to run LiveUpdate by hand once or twice a day until you download a new definition file, and maybe again the next day too, just in case there was a problem with the first definition file for the virus or worm.

(2) Prepare yourself:

This part is called **social engineering** and is the major reason why poorly designed worms and viruses — and most of them *are* poorly designed — can be so successful time after time after time. *Never, ever, open an email attachment unless you've asked the person who sent it to you whether he or she meant to send it to you.* Don't trust any sender. Don't blame them, either, if you get burned; these days it's not likely that the From: address has anything to do with the actual sender of the virus or worm.

Another essential precaution is to know what type of file you're opening. To do this in Windows, you have to turn on file extension viewing in Windows Explorer: open Windows Explorer, select **Tools** → **Folder Options** → **View**, uncheck **Hide file extensions for known file types**, click the **Reset all Folders** button, and click **OK**. Then if you're about to click on an **.exe** file, you'll know it. (Point your mouse at an attachment icon in Eudora, and the attachment's full filename, including directory, will

be displayed in the status bar at the bottom of the Eudora window.) Remember that Mimedefang adds **.txt** to the end of the filenames of all suspect filetypes, so look at their second extension also.

Principle Number 3: Don't download HTML Images.

You know those gigantic pictures that you get in spam email messages? Turning them off will save you from seeing the content of many spam messages even if you do accidentally open them. And it takes a lot less time to download these messages without the images; if you have a slow Internet connection, you will really appreciate the time and aggravation it saves you. And just think — no more disgusting pictures to look at!

Spam and wasted time aside, there are other types of HTML images in email messages, often ones that you can't see, that could be compromising your privacy — Web bugs. (Bugs as in hidden listening devices.) Web bugs are usually 1 pixel by 1 pixel in size and therefore you generally wouldn't see them. They are used to collect data about the person reading the email or, when they're on a Web page, the person or machine visiting the site. If you don't download HTML images, you won't download Web bugs. It's as simple as that.

Note that sending HTML images is not the same as sending HTML-formatted messages. Go ahead and do that if you feel you must. (Please don't send them to me, though; I prefer using my own fonts.) If you do feel the need to send HTML-formatted email, include a second copy in plain text also, for those people whose email programs can't handle HTML. They would probably rather get two copies — one in HTML and one plain text — than try to extract the email message's content from its HTML tags.

All set now for safe email viewing?

The boxes on this and the following page have the options you should set in Eudora and Outlook to help you do it. I suppose it's not terribly surprising that it's a lot easier to accomplish in Eudora than in Outlook. Eudora isn't intimately entangled with other programs and the operating system like Outlook is.

Comments are welcome; please send them to Judith Grobe Sachs, judygs@uic.edu

Eudora Options for Safe Viewing

Aside from social engineering — which is the most important ingredient — safe email viewing in Eudora is mostly a matter of setting a few options. Do this by selecting **Tools**, then **Options**, then the following **Categories**.

These are specifically for Windows; there are similar options for Macs.

Display:

Uncheck: **Automatically download HTML graphics**

(If you receive a message that you want to see the graphics in, say an advertisement from a store that you like to shop at, open the message, right-click in the message body, and select **Send to Browser** from the Context menu. Eudora will warn you of your folly and give you another chance to change your mind.)

Viewing Mail:

Message Window box:
Uncheck **Use Microsoft's viewer**

Preview Pane box:
Uncheck: **Show message preview pane**

Uncheck: **Automatically open next message**
Uncheck: **Allow executables in HTML content**

Extra Warnings:

Warn me when I:
Check **Launch a program from a message**
Check **Launch a program externally**

Miscellaneous:

Uncheck: **Say OK to alerts after xx Second(s)**

Safe Email Viewing in Outlook

The most important part of safe email viewing in Outlook is the same as in Eudora — social engineering — your being careful. In fact, it's much more important in Outlook than in Eudora because, unfortunately, Outlook doesn't offer quite as many ways to protect yourself from your own mistakes.

You can turn off the Preview Pane: **View** → **Preview Pane** toggles it on or off. The next item in the View menu, **Autopreview**, displays only the first three lines of messages, or of unread messages, depending on how you have it set up; don't use that either.

Now comes the problem. Your security choices in Outlook are tied to your security choices in Internet Explorer (at least). While you definitely don't want to execute Java or ActiveX in email messages, there are lots of Web pages that won't work properly if you don't allow them to run there. So you don't want to turn HTML executables off altogether.

I found a TechTV (<http://www.techtv.com>) Web page that had a really good idea on how to turn HTML executables off for Outlook but not for IE. They suggest setting Outlook up to use Window's Restricted Internet Security Zone, which in theory are sites that you don't trust at all. Turn off all the HTML executables for the Restricted Zone, which makes sense, and leave on whatever options you're comfortable with for the Internet Zone, which is mostly what Internet Explorer uses.

The instructions in the TechTV page are for Outlook Express. The real URL for the TechTV page is 76 characters, which is much too long for a printed page, but this "Tiny URL" will take you there: <http://tinyurl.com/xlxa> (I went to <http://tinyurl.com> and had them make the URL tiny for me!)

Here's how to do it for Outlook 2000 and Windows 2000, which is what I happen to have. Your Outlook and Windows will probably be slightly different; that's the way it is with Windows.

In Outlook, select **Tools** → **Options** → the **Security** tab, select the **Restricted Sites** zone from the dropdown list and click the **Zone Settings...** button. A warning dialog box will open telling you that the changes you're making will affect Outlook and IE and so on. Click **OK**.

This opens the Web content Security box, figure 1 below. You can change the settings for any of the security zones here, but we're only working on Restricted Sites, which will already be selected. You'd click the **Sites...** button to add specific sites to the Restricted sites zone, but in this case it doesn't matter whether there are any sites in the zone or not; we're only concerned with the security settings for the zone. So click **Custom Level...**

This opens the Security Settings box, figure 2 below. Select **Disable** or **Prompt** for all the Active X, Java, and Scripting options. If you want to turn everything off, you can select Reset to: **High** and click **Reset**. Then click **OK**, **OK**, and **OK**.

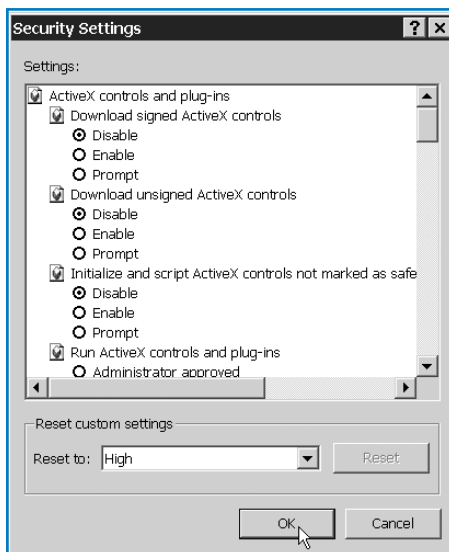
And now for the bad news. There does not appear to be any way to tell Outlook not to download HTML images. In fact, Microsoft says that it can't be done. But a colleague pointed me to a column in *TwinCities.com Pioneer Press* that gives a way to do it that involves editing the Windows registry. "Workaround stops e-mail pictures" by Jeffrey C. Kummer, *Pioneer Press* columnist, <http://tinyurl.com/ugs2>

Modifying the registry is definitely not for the timid; if you mess it up, your whole computer might not work. Unless you're confident about what you're doing, please don't do it.

Figure 1: Windows Security



Figure 2: Security Settings



Flu Shots for Your Computer

Tech Tips



Luckily for people, only fall and winter is flu season. Unluckily for computers, it's always flu season. But computers have a big advantage over us. Their flu shot is foolproof for flu strains over a few days old, and their flu shot manufacturer — in the case of UIC computers, Symantec — gets on top of new viruses and worms right away and distributes antiviruses for them generally within a day or so.

long as our we keep our site license, again at no cost.

We have a new version of SAV (for Windows*) and NAV (for Macs**) now; if you haven't installed it yet or you'd like to upgrade; now's a good time.

If you have any questions on SAV or NAV, go to the CSO or contact the consultants at consult@uic.edu.

* For Windows: SAV CE (Corporate Edition) 8.1 for Windows 98/Me/NT 4.0/2000/XP. SAV 8.1 doesn't support Windows 95, but version 7.61 of NAV is still available, which does. (You can't download it from home though.)

** For Apple Macintoshes running MacOS 8.1 through 9.x and MacOS X (10.1 or greater): NAV 8.0.

And also Novell and Windows NT/2000 Server Editions, which comes on a two CD set for \$15 per set. To purchase the CDs or for more information, please send email to software@uic.edu.

Installing Symantec Antivirus for Windows

- Uninstall any current antivirus program you might have, including previous versions of Norton AntiVirus:
 - Click on **Start** → **Settings** → **Control Panel**
 - Double-click **Add/Remove Programs**
 - Choose the program you want to uninstall, and select it to uninstall.
 - Reboot.
- Go to <http://www.accc.uic.edu/software/antivirus/win.html#Downloading>, and follow the instructions to download the self-extracting Zip file for Symantec AntiVirus (SAV). The download has been fixed so that you can now do it even from off-campus after identifying yourself by logging in with your netid and ACCC password with Bluestem.

The file is 34 MB, so it will take a while to download, particularly if you have a modem connection — a couple of hours. Even if the download does take hours, it will be hours well spent.

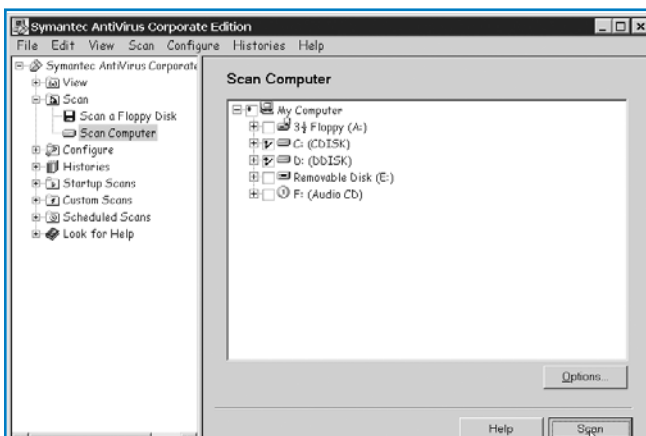
Figure 3: Running Windows LiveUpdate

Remember that you must be connected to the Internet to run LiveUpdate. Notice that LiveUpdate can update the LiveUpdate and antivirus program as well as the virus definitions.



Figure 4: Running a Manual Scan in Windows

Before you run a scan, click the **Options** button (lower right) to pick the scan options. The default settings will probably do; just click **Save Settings** then click **OK**.



And very luckily for us, UIC has a site license for Symantec AntiVirus (SAV), also and formerly known as Norton AntiVirus (NAV), which is widely agreed to be one of the very best antivirus programs around. Our site license allows any member of the UIC community to install Symantec or Norton AntiVirus on any of their computers, either here on campus or at home, for no charge, and also to receive updates for its antivirus definitions as

3. After the download finishes, go to the directory that you downloaded the file to and double-click on the **.exe** file you downloaded. The install program should start automatically. Read and accept the license agreement; then follow the instructions to install Symantec AntiVirus. If you use Microsoft Outlook or Lotus Notes for email, install their snap-ins, otherwise keep the suggested defaults, including running **Unmanaged** (unless it's for a machine at work and your department's REACH person tells you otherwise) and to install the **File System Realtime Protection**; they are correct for our use.
4. At the end of the installation, it will ask whether you want to run LiveUpdate when you finish and may ask you to restart your computer. Click **Yes** to both. LiveUpdate will either begin then or run automatically when your computer restarts. Keep the default connection method, by the Internet.
5. SAV's File System Realtime Protection inspects for known virus patterns on a continuous basis as you read or write files. It will also remind you if you shutdown your computer with a diskette in your floppy drive. The File System Realtime Protection will be started automatically every time you start Windows; you can see its yellow shield icon in the system tray on the Windows task bar at the bottom of your screen.
6. You shouldn't depend entirely on the Realtime File Protection, however. You should schedule regular scans of your entire hard drive.
 - a. Open Symantec AntiVirus: **Start** → **Programs** → **Symantec Client Security** → **Symantec AntiVirus Client**.
 - b. Click the **Scheduled Scans** in the left part of the window; if you reboot daily, you might use a startup scan, but the scan can get in the way of your using your computer.
 - c. Click **New Scheduled Scan**, type a name and description for the scan in the appropriate boxes, then click **Next** >.
 - d. Select Daily, Weekly, or Monthly and **select a time at which your computer will be running**. Click **Next** >.
 - e. Click in the boxes beside all of your local hard drives to select them for scanning, then click **Save**.
 - f. Click **Exit** to close Symantec Antivirus.
7. You should also schedule LiveUpdate to run on a regular basis. In SAV, select **File** → **Schedule Updates**, and click **Enable scheduled automatic updates**. Then click the **Schedule...** button. Run LiveUpdate at least weekly, and be sure to pick a time when your computer will be connected to the Internet. (See figure 5.) When you're finished, click **OK**, **OK**, and close SAV.

SAV does not have to be running for a scheduled scan to be running, but your computer does have to be on.

8. **If you're using Windows 95 or Windows 98**, make Emergency Rescue Disks as described in the "NAV Getting Started Guide" (see "Want to know more" below.) Make sure you write-protect the Emergency Rescue disks so you don't accidentally change them. Also, you will need to make new ones periodically so they'll have the newest virus definitions.

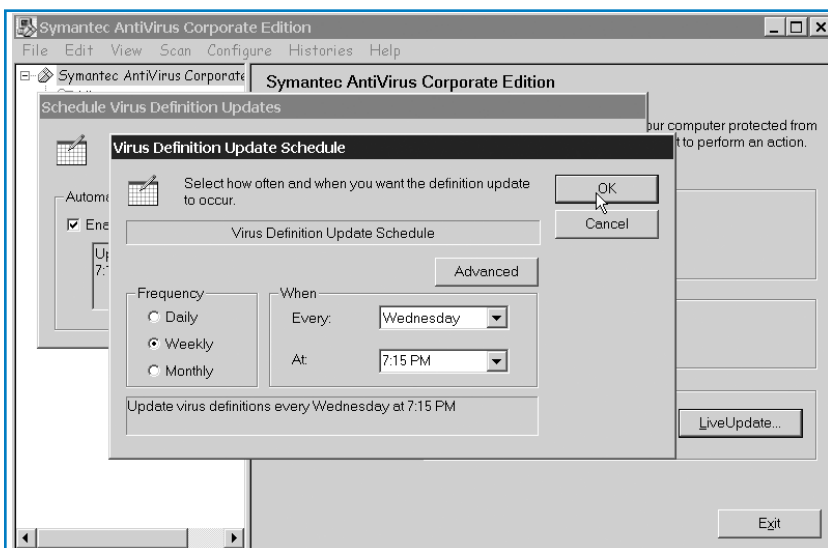
Want to know more?

Print the "NAV Getting Started Guide":

ftp://ftp.uic.edu/pub/antivirus/windows/docs/NAV7_QS.PDF. This four-page PDF will get you started. (NAV and SAV differ mostly in name.) There are links to it and other useful SAV user manuals in the Windows antivirus Web page at <http://www.accc.uic.edu/software/antivirus/windows.html>

Figure 5: Scheduling Regular LiveUpdates in Windows

Remember that you must be connected to the Internet to run LiveUpdate.



Installing NAV 8 for Macs

Got a Mac? We've got you covered too. Norton AntiVirus 8.0 for Macs. (Yep, the antivirus for Macs is still Norton.) Remember — our license agreement for Norton/Symantec AntiVirus allows it to be installed on any computer belonging to any member of the UIC community, whether it's on campus or off. Everyone at UIC should use it on all their computers, including Macs.

NAV 8.0 for Macs supports MacOS 8.1 through 9.x and MacOS X (10.1). In MacOS X, you must have administrator permissions and must enter your ID and password to install NAV, to run LiveUpdate manually, or to schedule automatic LiveUpdates. The account that scheduled the LiveUpdate has to be logged in to run it.

You will need the StuffIt Expander utility to uncompress the file you download. If you do not have it, you can download it from Aladdin Systems, Inc. (<http://www.aladdinsys.com/>).

1. Uninstall all other antivirus software you already have installed and restart your Mac.
2. Go to the Mac antivirus page, <http://www.acc.uic.edu/software/antivirus/mac.html>, and click on the **NAV 8.0 for Macintosh** link. The file is very large, so it will take a while to download, even on campus. We don't recommend that you try to download it from from home. Your best bet is to go to an ACCC lab with a Mac that has a CD burner and download it and write it on a CD there to take it home.

3. Your browser should have automatically uncompressed the file for you. If not, double-click the file name to expand into the same location.

4. Go to the directory where the file was saved, and double-click the "Install for" icon for your type of MacOS. Double-click the **Install Norton AntiVirus** icon. If you're installing on MacOS X, it will ask you to enter an administrator ID and password to authenticate the installation.

At the the Norton Antivirus welcome screen, click **Continue**. Read and **Accept** the license agreement, read the Read Me file, select **Easy Install**, then follow the prompts. Restart when you're asked to. Note that our access to LiveUpdate continues as long as our site license continues, not for just one year as the installer says.

5. After the Norton installer finishes and you restart your Mac, run LiveUpdate to update your virus definitions. If you get an error message about NAV when your reboot on MacOS X, ignore it; it should be fixed when your client gets updated when you run LiveUpdate. **LiveUpdate folder** → **LiveUpdate** → **Update Everything Now** button. (See figure 6.) If anything is updated, click **Restart** when LiveUpdate finishes. Remember that running LiveUpdate requires the computer to be on, Internet access, and, in MacOS X, the user who scheduled the LiveUpdate to be logged in.
6. Norton AntiVirus Auto-Protect protects files as you read and write them, including attachments in Eudora and Outlook. In MacOS 8/9, Auto-Protect comes automatically turned on (click the **Preferences** button to check; figure 7). In MacOS X, you have to turn it on if you want to use it. Click the **Preferences** button, click the **Auto-Protect** icon, then turn **Automatic Scanning** and **Automatic Repair** on. (Figure 8.)
7. Symantec says that you don't need to run NAV regularly if you run Auto-Protect all the time. But if you'd like to run it, start Norton AntiVirus by double-clicking the Norton AntiVirus icon. In the

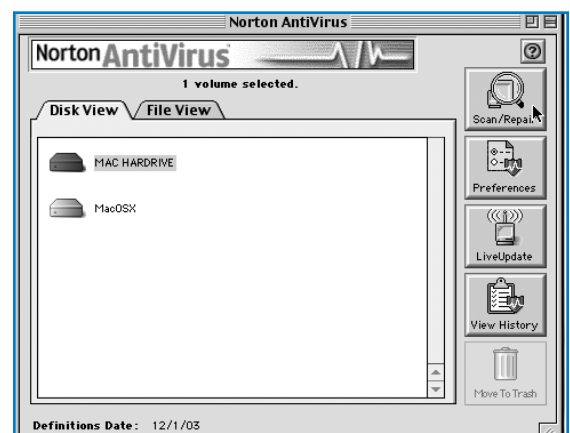
Figure 6: MacOS X LiveUpdate

Use **Update Everything Now** to run LiveUpdate and **Norton Scheduler** to schedule regular updates. The LiveUpdate main window looks and works very much the same in MacOS 8/9.



Figure 7: MacOS 8/9 NAV Scan

Select the files, folders, or disks you want to scan; then click **Scan/Repair**.



main window, select a disk, folder, or file to scan from the lists, and click **Scan/Repair** (figures 7 and 8). Or drag and drop a file or folder that you want to scan onto NAV. You can also schedule regular scan if you wish. For MacOS 8/9, start in NAV and select **Tools → Scheduler**. For MacOS X, click the **Scheduler** button; the folder you want to scan is “root”:

- It is important to keep your virus protection up-to-date by running LiveUpdate on a regular basis, say once a week.

Scheduling LiveUpdate for MacOS 8/9

- In the LiveUpdate main window, click **Schedule Future Updates**. This opens the LiveUpdate Scheduler window (figure 9).

Figure 8: MacOS X NAV Scan

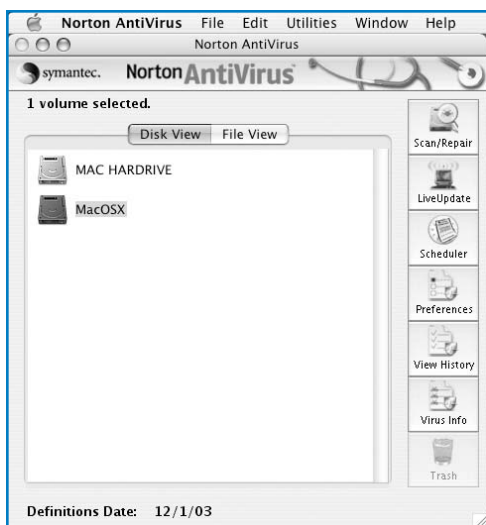
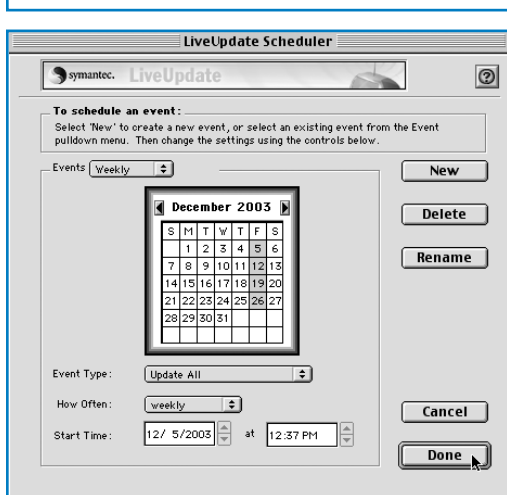


Figure 9: MacOS 8/9 LiveUpdate Scheduler

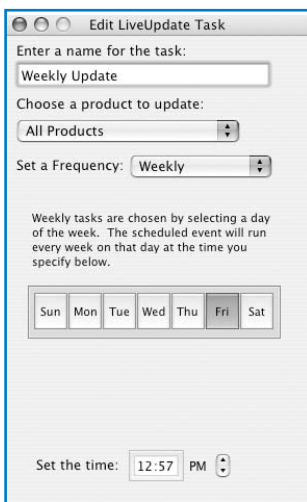


- Click **New** to create a new scheduled event. This opens a dialog box that allows you to enter a name for the event; in the figure, we've called it Weekly. Then click **OK**.

- Select **Update All** from the Event Type: dropdown list.
- Select **weekly** from the How Often: list.

- Select a time and date when the computer will be on and connected to the Internet.

Figure 10: MacOS X Liveupdate Scheduler



- Click **Done**.

Scheduling LiveUpdate for MacOS X

- In the NAV main window (figure 8), click **Scheduler**.
- Click the **LiveUpdate** icon to open the Add LiveUpdate Task window (figure 10).
- Enter a name for the task in the text box at the top.
- Select **All Products** as the products to update.
- Select a frequency; we recommend **Weekly**.
- Select a day and time when the Mac will be connected to the Internet and the person scheduling the LiveUpdate will be logged into it.
- Click the red button at the top left to close the window.
- In the Save LiveUpdate Task dialog box, click **Save** (figure 11).

Want to know more?

I can't offer you a short and sweet PDF file for SAV beginners, but there are links to Symantec's long and good user's guide and other useful manuals in the Mac antivirus Web page at <http://www.accc.uic.edu/software/antivirus/mac.html>.

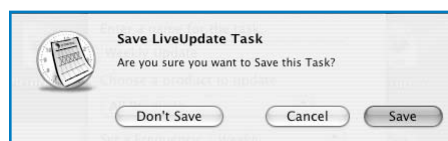
Northwestern University has a good, reasonably short how to install NAV for Macs (both versions) page at <http://www.tss.northwestern.edu/virus/nav-mac.html>.

Caution and a Good Antivirus Does Work

Whatever type of computer you have, whatever operating system, you owe it to yourself — and to the rest of us — to get and install antivirus software, run it all the time, and keep it up to date. Computer viruses are nasty, embarrassing things. You don't want to find out about them first hand.

Comments are welcome; please send them to Judith Grobe Sachs, judygs@uic.edu

Figure 11: MacOS X Save LiveUpdate Task Dialog



Securing Email & Editing PDFs

The Head Crash



Question: Hi, if I use Eudora from off campus are my password and email transfers secure?

Answer: If you are running IMAP or POP over SSL, which we support on mailserv, yes. The important part is protecting your password, which you only use when reading your email, so you need the SSL connection only when reading your mail. Note that “mail transfers,” either sending or receiving, are not high-security in any case. Having an SSL connection for this part doesn’t help a whole lot, because the mail will be transferred unencrypted from mail server to server, and will sit on the disk unencrypted. So either don’t worry about it (for most mail), or encrypt the mail yourself using PGP, GPG, or some other public-key program.

Bob Goldstein, ACCC Systems

Turning SSL on in Eudora: If you only have one “Persona” (account), then use **Tools** → **Options** → **Checking Mail**, then select **Required Alternate Port** from the dropdown list in the **Secure Sockets When Receiving** box on the right, then click **OK**.

If you have more than one Persona, then click the **Persona** tag (in the pane with the **Mailboxes** tab), right-click on the **Persona** for which you want to use SSL, click **Properties**, the **Incoming Mail** tab, and again select **Secure Sockets When Receiving**.

It would be nice if the **Last SSL Info** button would tell you whether SSL was turned on, but it doesn’t. You can tell by clicking on the spinning ying-yang when your email is being downloaded. This opens the Task Status window showing the progress of the download and it’ll say SSL while the mail is downloading. (Look fast!)

In Outlook: The ACCC doesn’t support Outlook for email, but here’s a hint. It’s an option on your **Mail** account, **SMTP** tab, **Server Requires Authentication**. How you get there depends on what type of Windows and Outlook you’re using.

Question: I have a PDF form that I need to edit. It was composed in Word and the form fields were created using Acrobat 5.0. Now I want to add/insert a line of text and form fields about three-fourths down the page. I’ve been unable to find instructions on how to do this in the Acrobat online help (I

looked under “insert,” “move,” etc.). Is there a way that I can edit the lower portion of the form without starting over? Thanks.

Answer: Acrobat Advanced Editing Tips:

To move printable items (text, lines, images), you use the arrow tool (“touch-up-object tool”), which is by default hidden behind the open-T tool (“touch-up-text tool”). You can move things by dragging or with the cursor keys (hold down **Control** to move them faster). When working with multiple pages, to move an object from one page to another, select it, then cut it (**Control-X**), move to the target page and paste (**Control-V**), then move it to the desired location (it will be exactly where it was on the source page). To select and move multiple items at once, you can hold **Control** down while clicking them or drag a rectangle over them. Warning: there are often invisible background objects (and objects often include other objects, especially after optimizing the document), so you might be selecting or moving too much.

To move form fields, use the form tool itself. While it is active, you can also duplicate (copy and paste) form fields for faster form creation.

To insert text, use the open-T tool (“touch-up-text tool”) and **Control-click** to start a new line of text. To change its attributes (e.g., font, point size), type the line, then right-click it and choose **Select Line**, then **Attributes**. Pick the font of your choice and hit **Tab** or **Enter** to commit. You can move the line sideways with its diamond-shaped handles at left, but up and down only by switching to the arrow tool.

Inserting graphics is not so straightforward. I occasionally do it by creating a separate PDF with just that graphic, then adding that page to my document (**Document** → **Insert Pages**, or just drag the thumbnails over), and finally moving the graphic where I want it before deleting the now unnecessary extra page. When trying to add lines it is much easier to play with the existing ones, making copies and moving those.

Hope this helps,

Volker Kleinschmidt
ACCC Instructional Technology Lab

The A3C Connection

Academic Computing and Communications Center (MC 135)
Room 124 Benjamin Goldberg Research Center
1940 West Taylor Street
Chicago, Illinois 60612-7352

About The A3C Connection

The A3C Connection is published four times per year by the UIC Academic Computing and Communications Center, providing news and information about the use of computers, communications, and networking at UIC. It is edited by Judith Grobe Sachs with help from the UIC Office of Publications Services.

Distribution of *The A3C Connection* is free to UIC faculty, staff, and students and to other universities and not-for-profit organizations. To subscribe, send us your name and address, UIC campus address if possible, including your department name and mail code. To cancel your subscription, send us your address label or a copy of all the information on it.

Contact us by electronic mail at connect@uic.edu; by telephone at the Client Service Office, (312) 413-0003; by U.S. Mail at *The A3C Connection*, ACCC (MC 135), Room 124 Benjamin Goldberg Research Center, University of Illinois at Chicago, 1940 West Taylor Street, Chicago, Illinois 60612-7352; or by fax at (312) 996-6834.

We welcome any comments, suggestions, complaints, or requests you might have concerning *The A3C Connection*.

The Fine Print

The use of trade, firm, or corporation names in this publication is for the information and convenience of the reader. Such use does not constitute an official endorsement or approval by the University of Illinois of any product or service to the exclusion of others that may be suitable. Trade names that may appear in this publication include the following: Apple, the Apple logo, Mac, Mac logo, and Macintosh (registered trademarks of Apple Computer, Inc.); AIX and AIX/ESA (registered trademarks of IBM Corp.); UNIX (registered trademark of The Open Group); HP and HP-UX (registered trademarks of Hewlett-Packard Corporation); Sun, Solaris, and Java (registered trademarks of Sun Microsystems, Inc.); and Microsoft, Windows, Windows NT, and other Microsoft product names (trademarks or registered trademarks of Microsoft Corporation). All other product names mentioned herein are used for identification purposes only, and may be the trademarks or registered trademarks of their respective companies.

Permission is granted to reprint or adapt all or part of *The A3C Connection* for nonprofit use, provided that full acknowledgment of the source is given.