

## *CIS Survey Results*

This summer Computing and Information Services conducted a survey of faculty and staff. Our main goals in sending out the survey were to evaluate the effectiveness of our Help Desk and to get input on our workshop program. We also wanted to know whether there were services that we are not currently providing that users would like to see added.



We received responses from 49 people: 7 academic support staff, 23 administrative staff, and 19 faculty. In general we were very pleased by the results of the survey. The majority of users who responded felt that the Help Desk staff were helpful and friendly and were able to respond to their problems promptly. We were somewhat disappointed by the inconsistent use of the Help Desk phone number, however. Only 9 users reported using the Help Desk phone number as their primary means of reporting a problem. Calling a CIS staff member directly was the most popular way of reporting problems. We do seem to be doing a good job in terms of giving notice of when we make changes: 43 of the 49 responders said that we give plenty of notice. Only one user said we don't give enough notice and 5 did not answer this question.

When it came to types of problems reported by users, "my computer" was the most frequent single source of problems, but many users reported having problems with some combination of their computer, the network, a server, and/or software.

We received many helpful comments on our workshop program. While people who were able to attend workshops generally found them to be helpful, many users reported that they were often not able to attend workshops due to conflicts in their schedule. This semester we are trying to address this problem by offering multiple sessions of the same workshops at different times of day and on different days of the week. We also got many ideas for new workshops on other topics. More multimedia software and more advanced Microsoft Office workshops were the most commonly asked for workshops. We will definitely keep these suggestions in mind when we develop new workshops for next summer.

Surprisingly, we did not get many suggestions on new services that we might offer. Several users mentioned enjoying *Occasional Downtime* and we appreciate that feedback.

Many thanks to everyone who responded to our survey. We value all of our users' comments. 🐾



# CARS Update

## IN THIS ISSUE

CIS Survey Results -----	cover
CARS Update -----	2
Editor's Notes -----	3
Recent Computer Virus Activity on Campus -----	4
Tricks & Tips -----	7
Q&A -----	8

For many of us at the Claremont Colleges the CARS implementation project still seems somewhat unreal. We know that the Claremont Colleges have purchased a new student information system and that we are in the process of implementing it, but not many of us have been personally affected by the project yet. This will change in the not-so-far-off future. The Project Implementation Teams and Campus Project Managers have been increasingly busy converting data, training on CARS and the new reporting tools, and generally getting ready to meet upcoming deadlines. In addition, "Tiger Teams" have been formed for each functional area to test the baseline system and the customizations we have requested. Tiger Team members are generally power users of the current systems and knowledgeable about their office needs. The teams are usually made up of one office representative from each college. They are receiving training early so that they can test the system and verify that the data is being converted correctly. They are also working on setting up code tables and configuring the options for the new system.

The process of going live with a module begins with installation of the "baseline" software, essentially the out-of-the-box version of the CARS software. CARS then installs custom modifications requested by the Claremont Colleges. Testing of the module and training of the Tiger Team is done at this stage. After testing, CARS installs any additional customizations requested by the individual colleges. Data conversion is going on at the same time the modules are being implemented so that the Tiger Teams can test the system with real data. The IT staffs of each college are working to convert the data from their

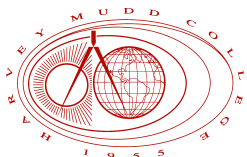
current database system to the new CARS system. After all of the customizations are in place and final testing has occurred, the functional staff who will use the CARS system will be trained. Then there will be a final dump of the data from the current system just before each module goes live.

This is the general outline of the process of implementing one of the CARS modules. Not every module will follow it exactly. For example, the registration module, which will be the first to "go live", will actually be implemented in two stages. "REG I," which includes course scheduling and registration, will go live in March 2002 in time for Fall 2002 student pre-registration. Graduation reporting and tracking of this year's seniors will take place using the current database system. "REG II," which includes grade tracking and reporting, will then go live in June 2002.

The other modules (Student Services/ Career Services, Financial Aid, Student Billing, Institutional Advancement (Development), and Admissions) are scheduled to go live over the course of the following year and a half. Student Services and Career Services will go live in May 2002, Student Billing in June 2002, Financial Aid in November 2002, Institutional Advancement in February 2003, and Admissions in February 2003. These dates are tentative, of course, and may change during the course of implementation.

In addition to training on the CARS software, many staff members will also be receiving training on the Cognos reporting tools PowerPlay and Impromptu. IT staff and Tiger Team members are being trained

*Occasional Downtime* is composed on a Macintosh G3 computer using Adobe PageMaker 6.5 and Microsoft Excel 98. The primary typefaces used are Times and Optima. We wish to thank Sally Rich Arroyo of the HMC Office of College Relations for all her help.



now in basic and advanced reporting so that they can help other staff later. All functional staff who do reports or ad hoc queries will receive training on the reporting tools as their modules near the go-live date. The Cognos tools can easily be used to generate simple reports while complex reports and “what if” scenarios can be developed with the help of IT staff.

In other CARS news, the Claremont Colleges have purchased Track-It!, a help desk software package which will be used to manage user support of the CARS student information system. The Claremont Colleges are planning on running a centralized CARS help desk to handle user support related to the CARS database. CIS will continue to support HMC users with respect to the installation and use of the CARS client software on users’ desktops. Users will always be able to call the CIS Help Desk for help with the CARS system. If the Help Desk staff cannot answer the question, they will be able to route it to the main CARS Help Desk.

Track-It! is also being evaluated by some of the colleges, including HMC, as a system for tracking general user support. At HMC we are in the process of hiring a Help Desk Support Specialist, a new position at CIS. The Help Desk Support Specialist will be in charge of our frontline Help Desk and will answer the Help Desk phone line, greet walk-in customers, and log and dispatch calls in the Help Desk database. We should have more news on our new position and the Track-It! help desk database later this year. 🐾



## Editor's Notes

The fall semester is flying by for all of us, the editor of *Occasional Downtime* included! October turned into November all too quickly and somehow the October issue of *Occasional Downtime* has become the October/December issue.

In any case we have an issue full of relevant articles. Our cover article is a brief summary of the results of a survey we recently took of faculty and staff. The survey results have really helped us consolidate our plans for the CIS Help Desk and gave us many ideas for our workshop program as well.

It's been a while since we reported on the progress of the implementation of the new student information system, CARS. Our second article describes recent progress in the implementation project and a bit of what users can expect in the coming months. Our final article covers recent virus activity at the Claremont Colleges. Nimda, Code Red, and Sircam are all viruses that have made their presence felt lately.

—Elizabeth Hodas

---

*Occasional Downtime* is published five times a year by the Computing and Information Services Department at Harvey Mudd College. It is also available in PDF format on the HMC Web Server. Comments and questions can be directed to [downtime@hmc.edu](mailto:downtime@hmc.edu).

# Recent Computer Virus Activity on Campus

Computer viruses have certainly been in the news lately. Several new viruses recently became widespread throughout the world and had a significant impact at the Claremont Colleges as well. Although we published an article about computer viruses quite recently (*“Everything You Always Wanted to Know About Computer Viruses—But Were Afraid to Ask,”* Volume 9, Issue 1, February 2001) it’s worth discussing these recent viruses because they use new and different ways of spreading.

Nimda is the latest virus to hit the Claremont Colleges. Nimda first appeared on September 18, 2001 and spread quickly.

At the Claremont Colleges the main effect was increased network traffic caused by the virus scanning IP addresses searching for Microsoft IIS Web servers to infect. Several colleges were forced to take down some of their servers. Guido, the network traffic shaper, was also incapacitated due to the increased network traffic.

Nimda (from “Admin” spelled backwards) is a particularly complex virus in that it spreads in not one, or even two, but in four different ways. The virus affects Windows 95, Windows 98, Windows Me, Windows NT 4 and Windows 2000 users. Initial infection by the virus is primarily by an infected attachment, usually named

README.EXE. The subject line of the email message varies and the body of the message is blank. Opening the attachment executes the virus. Simply viewing the message in Microsoft Outlook or Microsoft Outlook Express using the preview pane feature can infect a user’s machine.



Once a machine is infected the virus spreads in four different ways:

▼ Mass mailing: Like many other recent viruses, Nimda will send a copy of itself to all email addresses it finds in the user’s MAPI-compliant email client. This includes Microsoft Outlook and Outlook Express. In addition, Nimda

searches for email addresses in all local .HTM and .HTML files and sends copies of itself to those addresses as well.

▼ File infection: Nimda infects some .EXE files by embedding a copy of itself inside the executable file. The virus can thus be spread by users who exchange executable files such as games.

▼ Web server infection: Nimda scans randomly generated IP addresses on the Internet searching for Microsoft IIS Web servers. If it finds an IIS server that has not been patched against the Microsoft Directory Transversal

Vulnerability, it infects the Web server and modifies files named DEFAULT, INDEX, MAIN or README, or files with the extensions .HTM, .HTML, or .ASP by adding JavaScript code. The JavaScript code opens a Web browser window with the infected file README.EML, which is an Outlook Express email file with the virus as an attachment. Users who access these infected Web pages using an unpatched version of Internet Explorer may then become infected by the virus.

▼ File sharing:

The virus also looks for open network shares by searching through the Network Neighborhood. Nimda creates .EML files in any shared directories that the user has access to. It also copies a hidden file called RICHEL20.DLL into any directory that has .DOC and .EML files. When other users try to open .DOC or .EML files from these directories, Microsoft Word, Wordpad or Microsoft Outlook will execute this file, causing infection of the user's PC.

As previously mentioned, increased network traffic was the main impact of this virus at the Claremont Colleges. However, proliferation of infected files on file servers, such as our Novell file server *Kato*, was also a significant problem.

Two other viruses seen at the Claremont Colleges were Code Red and Code Red II. The original Code Red worm was discovered on July 16, 2001. It exploited a security hole in the Microsoft IIS Web server. The worm had several phases, repeated on a monthly basis. During the "infection phase" infected servers would attempt to infect other Web servers by scanning IP addresses. This was followed by a phase where the worm would initiate a denial-of-service attack against [www1.whitehouse.gov](http://www1.whitehouse.gov) (the address of the White House's Web site was quickly changed in response). This was followed by a "sleep" phase until the next month rolled around. In addition the worm would

sometimes change the home page of the infected Web server to read: "Welcome to <http://www.worm.com>! Hacked by Chinese!"

Code Red II was discovered on August 4, 2001. It is a variant of the original Code Red worm in that it exploits the same security hole in the Microsoft IIS Web server software. Infected Web servers scan for additional servers to infect, but the worm also installs what is called a "backdoor." This backdoor allows hackers to have full remote access to the Web server. When scanning for Microsoft IIS Web servers, Nimda actively searches for servers that have this backdoor installed by the Code Red II worm.

The Code Red worms were the first to spread in this particular way and they spread around the world remarkably quickly. On July 19, 2001 over 359,000 computers were infected by the Code Red worm in less than 14 hours. Both viruses caused significant network traffic at the Claremont Colleges and several colleges were forced to take servers down.

Another virus that had a significant impact at the Claremont Colleges was the Sircam virus. Sircam is a relatively typical email mass mailing virus that spreads in the form of infected email attachments and infects Windows computers. Once a user opens an infected attachment, their machine is infected by the virus. The virus then spreads by sending infected copies of documents found on the user's machine to email addresses found in the Windows Address Book and in temporary cached Internet files. The filename of the infected attachment will thus vary, although the attachment will always have a double extension (such as .DOC.PIF or .XLS.LNK). Because the virus sends documents from the user's machine, it may release confidential user information. The virus may also infect other systems by copying itself to open network shares and

(continued on page 6)

may delete files on the user's machine. CIS had many reports of users receiving the Sircam virus. Fortunately, most were caught by the demo anti-virus software installed on Thuban and HMCADM, the two mail servers for faculty and staff.

Given how quickly these new viruses spread, what can users do to protect themselves and their community? Here are a few simple tips:

▼ Be wary of all email attachments that you receive. Because mass mailing viruses use email addresses collected from infected users' machines, an infected attachment may be sent to you by someone you know without their knowledge. If you are not expecting an attachment from someone, think twice before opening it! Check back with the sender and/or search one of the antivirus Web sites before proceeding.

▼ If you do receive an infected attachment, be sure to delete the infected document from your attachments directory as well as the email message. Contact the Help Desk at [help-desk@hmc.edu](mailto:help-desk@hmc.edu) or at extension 7-7777 if you need help deleting the attachment.

▼ Install antivirus software on your computer and keep it up to date. CIS has Virex for the Macintosh and McAfee VirusScan for faculty and staff. If one of these products is not installed on your machine contact the Help Desk. We have also been testing antivirus software on Thuban and HMCADM which we may purchase and install on all of our mail servers.

▼ Do not forward virus warnings to the community. Many of these virus warnings that you receive by email are actually hoaxes. Send them to the Help Desk first. We'll be happy to confirm or deny them for you.

## SOURCES

CAIDA (Cooperative Association for Internet Data Analysis): The Spread of the Code-Red Worm (CRv2)

[http://www.caida.org/analysis/security/code-red/coderedv2\\_analysis.xml](http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml)

F-Secure Virus Descriptions

<http://www.datafellows.fi/v-descs/>

McAfee Virus Information Library

<http://vil.mcafee.com/>

Andrew Mackie et al., "Nimda Worm Analysis", Incident Analysis Report, Version 2, September 21, 2001, Security Focus, 2001.

Sophos Virus Info

<http://www.sophos.com/virusinfo/>

Symantec Security Response

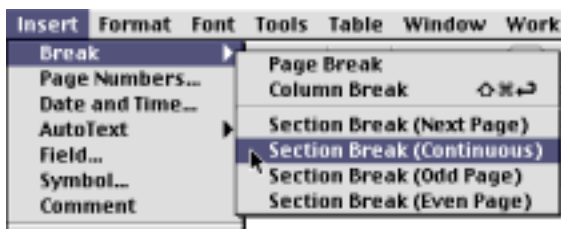
<http://www.symantec.com/avcenter/>

▼ Microsoft has published patches for the security holes in Internet Explorer 5.1 and 5.5 and in IIS 4.0 and 5.0. They are located at <http://www.microsoft.com/technet/security/bulletin/MS01-020.asp> and <http://www.microsoft.com/technet/security/bulletin/ms00-078.asp>, respectively. 🐾

## SECTIONS IN MS WORD

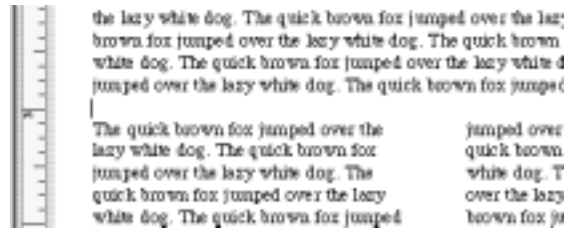
Sections are used in Microsoft Word for a variety of reasons. One of their main uses is to designate different page formats. For example when you switch from single-column to two-column mode you need to insert a new section. Then, when you want to switch back to single column mode, you'll need to insert another new section. Sections can also be used when you want to create different headers and/or footers for some pages in your document.

Let's use the example of switching from single-column to two-column mode. After typing the text you want in single-column mode, you'll create a new section for the two-column portion of your document. Select "Break/Section Break" from the Insert menu. There are four types of section breaks you can choose from: "Next Page", "Continuous", "Even Page", and "Odd Page". "Next Page" creates a new section on the next page. "Continuous" creates a new section at the insertion point. "Even Page" creates a new section on the next even-numbered page and "Odd Page" creates a new section on the next odd-numbered page. "Next Page" and "Continuous" are the options you will probably use most often.



For this example, select "Continuous" to create a new section at the insertion point. Then select "Format/Columns" and click the Two button to switch to two-column mode. Type the text you want in two-column mode. When you're done insert another continuous section break from the Insert menu. Then switch back to single-column mode by selecting "Columns" from the Format menu.

# Tricks & Tips



In Page Layout mode your document should look like the screen shot above: In Normal view mode you will be able to see the section breaks that you have inserted as in the screen shot below:



To create different headers or footers for some pages simply insert a section break. You'll want to use the "Next Page" option this time. Then use the "View/Header and Footer" command to view your headers and footers. One of the buttons on the header and footer toolbar is the "Same as Previous" button. Make sure this button is unchecked so that you can type a different



header or footer from the previous one. Then go ahead and type a different header or footer for this section. When you're done, close the header and footer toolbar.

You'll find many other applications for sections once you get used to using them!



# QUESTIONS *and* ANSWERS

---

**Q:** When I try to launch Eudora on my PC, a dialog box opens that says there is a remote instance of Eudora running, and gives the option to terminate the remote instance or quit. Neither of these options get Eudora to launch.

**A:** Eudora is not designed to allow multiple users to access its files simultaneously; it has no mechanisms to protect files from being corrupted when accessed simultaneously by multiple users. You also can not run multiple instances of Eudora at the same time with the same mailboxes. If you are not trying to open Eudora multiple times to access the same files, then you may be getting this error after a crash. When Eudora is launched on a PC, it creates an Owner.lok file, and gives you the warning about a remote instance if that file is found already existing in the Eudora directory. Crashing out of Eudora doesn't give it the opportunity to clean up after itself and sometimes leaves a corrupted Owner.lok file. Delete this file and you should be able to open Eudora again without the remote instance dialog box.

To delete the Owner.lok file first quit Eudora. Then locate your Eudora mail directory. For administrative staff users the mail directory should be located on their H: drive. Other users may have their mail directory on their H: drive or on their C: drive. Open the mail directory and locate the Owner.lok file. Delete the file by dragging it to the Recycle bin.

**Q:** Someone sent me a Microsoft Word document as a Eudora email attachment. I can open the document

and make changes to it, but how do I send it back to my colleague?

**A:** Eudora makes it pretty easy to open attachments. As long as Eudora can figure out what the file type of the document is, and you actually have the application needed to open the file, you can open the document by simply double-clicking on the document's icon at the end of the email message. If you need to edit the file it's best to use the "Save As..." command to save your changes and give the document a different name. This has two advantages: you keep a copy of the original document and when you send the document back, your colleague won't confuse their original file with the one you've just edited.

To send the document back as an attachment you need to know where the file is located. Eudora usually stores attachments in a special attachments directory. In the Windows version of Eudora the Attach directory will either be in your Eudora directory on your C: drive or in the Mail directory on your H: drive. In the Macintosh version of Eudora the Attachments directory is usually in the Eudora folder in your System Folder.

To attach the file from Eudora, create a new message or reply to the original message and select the "Attach File" (Windows) or "Attach Document" (Macintosh) command from the Message menu. Navigate to the attachments directory and select the file you want to attach. You can then enter a message in the body of the email and send it as you normally would. 📎