Benchmarks Online

Volume 3 - Number 5 * May 2000

Columns

Other Resources

Feature Articles

Campus Computing News

The "love bug" bit UNT this month, with a vengeance. Read Dr. Leatherbury's ILOVEYOU diary and reap the benefits of his experience.

Renew PRAS Accounts for the Summer

You will need to renew your **P**remium **R**emote **A**ccess **S**ervice subscription if you only paid through the spring semester and you want to keep it through the summer. You may also need to take action to ensure the continuation of your UNT Internet Account, under certain circumstances.

Need Statistics for Your Website?

If you have a Website that is hosted by Central Web Support at UNT, you can get a detailed statistical report of Web use for that site.

Save a Tree. . . .E-mail Your Homework

Did you know that the General Access Labs have printing policies? Well they do, and they're not just for students either.

Virus Protection Means Never Having to Say You're Sorry

Subscribe to Benchmarks *Online*

Protecting your computer from viruses just might mean never having to say you're sorry. Read this article to find out how to get automatic VirusScan updates for your home computer and what "Crispen's Six Antivirus Rules" are.

HTML Formatting in GroupWise 5.5

Did you know that the GroupWise 5.5 extended client allows you to "webify" your E-mail? Now your mail messages can be just as colorful and creative as a Web page.

GroupWise Document Management: Checking Documents In and Out

This is the fourth in a series of articles on the topic of GroupWise Document Management.

Don't forget to check out our monthly columns. This month's topics:

- **RSS Matters** -- "Web Survey DIY"
- **The Network Connection** -- "Who do you trust?"
- **List of the Month** -- "BugNet"
- **WWW@UNT.EDU** -- "Security on the Internet"
- **Short Courses** -- Update on the various training opportunities on campus.
- **IRC News** -- Minutes of the April 18 and May 9, 2000 meetings.
- **Staff Activities** -- New employees, employees that have resigned, and staff awards and recognition are included in this article.

Research and Statistical Support
University of North Texas

RSS Matters

By Dr.Karl Ho, Research and Statistical Support Services Manager

Web Survey DIY

A graduate student came to me about four years ago and asked me to help her to launch a survey. Touched by her enthusiasm and genuine interest in an academic topic, I laid out the game plan for her to follow through: first identify your goal and target respondents (say, a sample of 300), draft the questionnaire and carefully word and order the questions, then pilot test the instrument and revise it from the preliminary test, print the finalized version and send them off..... Out of empathy with the student's budget and time constraint, I subconsciously cut short the process and try to make it workable for her. When she found out the amount of work that would be involved, she started to ask me: "Can I pay someone to do that for me?" "Yes", I replied and I referred her to some professional services. Very soon, she came back, disappointed, and asked me to give her the list again. Clearly, she was frustrated by the price tag of doing survey via professional services out there.

Not an uncommon situation, but I feel for the researcher every single time, particularly students who usually have a petit budget for doing first-hand survey. Not every research project can find funding from a big external fund or endowment such as the National Science Foundation. In fact, in a lot of cases, it is not necessary to have big money to do high-power research (remember Richard Feynman's O-ring experiment?). In fact, we have some new options.

A new support area for survey researchers

With the advent of the Internet and optical recognition technology, we have recently developed and opened a new support area for survey researchers. The services we can provide in this new area include:

1. Web survey consulting
2. Questionnaire design
3. Survey data preparation
4. Project planning

We have acquired two new software packages to provide tools for researchers to do surveys on their own. TELEform is a suite of applications that help in almost every procedure in a questionnaire-type survey. It includes designing the

questionnaire, rendering the instrument as a scannable form or an interactive Portable Document Format (PDF) file, verifying returned questionnaire and automated entry of data into SPSS, Excel or SAS formats. A high-speed scanner is in place to process high-volume scanning while professional data entry specialists can assist with the verification and data conversion process.

The other software, SurveySolutions for the Web, helps researchers to convert a questionnaire on word processor format into Microsoft FrontPage forms. We currently have short courses that train users to design FrontPage Web surveys. With SurveySolutions for the Web, we can now help customers to easily convert a questionnaire in Word or WordPerfect format into a FrontPage form to be posted on the Web. For more details on the Web survey process, check out my class notes at: New Technologies for Survey Research

Equipped with these new tools, we hope to provide more versatility and a wider spectrum of functionalities for survey researchers. Researchers can stick to the old methods and print out professional looking questionnaires for face-to-face interviews or to be mailed to respondents. When these questionnaires are returned, we can send it to the scanner connected to the TELEform server where the verification and data entry process begins.

Alternatively, the researcher can convert the file into a PDF file and post it on the Internet. Responses will be received at the Web server and be rerouted to the TELEform server. For researchers who only have a small budget and/or want to focus on respondents who have access to the Internet, a Web survey will suffice and the response rate is usually higher.

All that being said, technology alone does not preclude the key elements of survey research such as planning, sample selection, crafting of questions, etc. Observing that mediocre research prevails on the Web, we advise prudence. A highly sophisticated Web survey will not necessarily produce good findings, neither does technology always bring good stuff. With poor planning and administration, the effort and time invested can be turned into bad and even misleading findings.

Karl's tips on administering a survey

In the following I provide some links to tips on administering a survey, that I consider helpful for survey researchers:

RSS short courses: New Technologies for Survey Research I & II
Perseus* white paper: Survey 101- A Complete Guide to a Successful Survey
Perseus white paper: Seven Steps to a Successful Web Survey
SPSS: Guidelines for creating better questionnaires
SAS: Sample Survey Design and Analysis

Again, it is always advisable to plan early. Contact us should you want to launch a survey yourself. Rich Herrington has just returned from a training in TELEform designer. With his new expertise, we look forward to helping researchers tap into the new technology we have recently acquired.

Rich Herrington:

Phone: 565-2140

Email: richherr@unt.edu

Karl Ho

Phone: 565-4066
Email: kho@unt.edu

---

* Perseus is the developer of SurveySolutions for the Web

Network Connection

By Dr. Philip Baczewski, Associate Director of Academic Computing

Who do you trust?

Thanks to the "ILOVEYOU" virus, obnoxiously nicknamed "the love bug" by the popular press, we are now again aware of the tenuous status of our computers' ability to live on the Internet as well as continue to function from day to day. That is, some may feel a bit shaken, however, others seem as confident as clams in the mud. Is it just a matter of time until your luck runs out? Is it just a matter of odds? Maybe, but maybe not.*

Some of the ways to avoid the ILOVEYOU virus are to use a Macintosh or LINUX operating system, use Windows but not its E-mail subsystem, or just not open any attachments for which you don't recognize the file type or file origin.The reason the ILOVEYOU virus spread at all was because of the trust people placed in the source of the message and its integrity. The other reason was that it was so easy to exploit the interoperation of the Windows operating system and some of its tightly integrated programs.

The View Through the Windows

It's interesting to note that Microsoft's initial reaction to the ILOVEYOU virus was to do nothing. Their stance was that there wasn't any kind of bug in their software, so they didn't need to release a patch or anything. That's the scary part. The software was working the way it was supposed to work. In other words, it is a feature of Windows to allow an unknown program to access your address book, send out E-mail, and write over your files, all without any knowledge or intervention on your part. Microsoft claims that these are features that their customers required.

Act II of this drama is that Microsoft recently released a patch for their Outlook Express E-mail software. If the patch is applied, Windows will prompt you for your approval before letting a program do things like access your address book. Microsoft states that this may be an inconvenience for people used to doing automated contact acquisition and the like functions. Apparently, letting a program trash all your files is not considered an inconvenience by those geniuses at Microsoft.

It's so Convenient

So, you ask, what's wrong with a little convenience? Doesn't Microsoft just want to make things easy for us? You bet they do. They can make a whole lot of things easy. That's why they would enable an E-mail attachment with a "VBS" extension (for Visual Basic Script) to run as soon as you open it. This let's your E-mail talk to your Internet browser, or your word processor. It just happens that all of those things are made by Microsoft.

Microsoft wants to make things easy and convenient so that you won't have to know anything about computing. This is in your best interest isn't it? Well it does make you rather dependent on using Microsoft's operating system, Microsoft's browser, Microsoft's E-mail program, Microsoft's word processor, etc. But it's so convenient!

Protection Money

Microsoft makes things so convenient that you don't really need to understand computing to use it. But that's OK, because you can buy a third-party virus protection program and keep your computer safe, right? Even the best virus protection programs didn't stop some bright people from "catching" and perpetuating the ILOVEYOU virus. Virus protection programs are by necessity reactionary. You can't make a vaccine if you don't have a sample of the virus. There is always a lag, however short, between the appearance of a new virus and measures to control its spread. This is true whether you are talking about computers or humans.

A virus protection program can guard you against the accidental infection, but it doesn't protect you against the unknown. The virus protection companies would like you to believe that all you have to do is use their product and keep your virus data up to date and you'll be safe. They make a lot of money because you believe that. It's not that their programs don't have utility, but you do have to ask whose best interest do they really have at heart?

A Matter of Trust

So who do you trust? Microsoft? McAfee? How about yourself? The ILOVEYOU virus could have been defeated by healthy doses of skepticism. This is true of other similar viruses. Did that "South Park" attachment really come from your 90-year old Aunt Millie? Does the high-speed networking mailing list really love you? If you don't know what a ".VBS" file is, should you try to view it? If something looks like garbage mail, could it be?

If you put your trust in Microsoft or other commercial companies that have a vested monetary interest in your ignorance, you will get what you pay for. Or rather will pay dearly for what you get. You will pay by losing your independence. Here's where a little education can go a long way. Keep up with current trends in computing. Know all of what a program does before you install it. Know what the new features of an operating system are before you upgrade. Or better yet, free yourself from software profiteers by adopting open source operating systems and programs (but be prepared to do some serious learning). Oh, and one more thing -- is your hard drive backed up?

Comments, Questions? Send them to Philip Baczewski.

Other articles in this issue also address the topic of viruses and computer security:

- "Campus Computing News"
- "Virus Protection Means Never Having to Say You're Sorry"
- List of the Month -- "BugNet"
- WWW@UNT.EDU -- "Security on the Internet"

List of the Month

Each month we highlight one Internet, USENET Special Interest Group (SIG), or similar mailing list or Website.

One of the major news topics this month has been the ILOVEYOU virus and it's cousins. It seems fitting, therefore, that the Bug Net newsletter should be our May "List of the Month." Bug Net bills itself as the leading provider of software bug fixes, and software bugs are frequently they way virus authors get their programs to perform dastardly deeds.*

Bug Net charges for their services, but they offer a free newsletter and there is lots of free information available on their Website -- http://www.bugnet.com/ From this page you can subscribe to the newsletter, and read bug alerts and FAQs. It is a good place to become aware of fixes that are available for your favorite software, oftentimes free from the software vendor.

Other articles in this issue also address the topic of viruses and computer security:

- "Campus Computing News"
- "Virus Protection Means Never Having to Say You're Sorry"
- The Network Connection -- "Who do you trust?"
- WWW@UNT.EDU -- "Security on the Internet"

WWW@UNT.EDU

By Mark Wilcox, Campus Web Administrator

Security on the Internet

The past few weeks have been busy ones in the Internet security arena. We've seen more press and more people have been affected than ever before, including here at UNT.

While the monetary damages may be open for debate, in reality, most of us know someone who's been affected by things like the ILOVEYOU virus, credit card fraud or similar vile things.*

The first response to this shouldn't be "make more laws". For the most part, the laws we have are workable for the crimes that are committed. In reality what is needed is to make computer software companies more liable for the security risks they enable and we, the consumer need to punish those companies that don't by not doing business with them.

Second, we should use more common sense when using computers and computer security products. If you have a lock on a door, do you start telling everyone you don't need police or if you have a sprinkler system do you tell people that you don't need a fire department? Of course not, but this is exactly what we do when we put all of our faith in computer security products.

After all, locks on doors only provide us with is a deterrent, meaning we're telling a 'home hacker' (AKA burglar) to go look for some place easier to steal from. Locks and sprinkler systems offer us more time to respond in case of a break in or a fire.

However, most computer security companies try to lull us into believing all we need is their products and nothing else. They say their products will protect us against any computer evil without needing any type of response. This is just plain stupid. Of course we need a response, any system is vulnerable to an attack. What we need are ways to make a planned response and for these systems to buy us more time to respond when something does happen. In other words we need to have the same expectations of security products as we do of our other security systems like door locks and alarm systems. While this won't necessarily solve all of our ills, it will be a step in the right direction.

Until next time.

Mark

The humorist James Lileks gives his take of the situation in a column that appeared in a variety of places including *The Cincinnati Post* (http://www.cincypost.com/opinion/lileks051500.html) -- Ed.:

> Someday we'll love hackers
> Column by James Lileks
> . . .
> The news media love these virus stories. They have a familiar shape

now. First, the discovery, fraught with warnings - this could be as big as Melissa! Of course, no one has any real sense of how "big" Melissa was. Badness is now defined as how long a story occupies the top-of-the-hour news. Badness now means nothing more than: "You'll be hearing about this long after you're sick of it."

Next, tales from the victims. "We can't send or read any e-mail! It's horrible! The boss sent an officewide message about the Stapler Procurement Committee, and no one can read it!" Oh, the humanity.

Then, the What it Means portion. By "Nightline" time, the experts and sociologists assemble to drone and intone on the usual issues - Our Increasing Vulnerability, the Irony of Our Vulnerable Interconnectedness, the Price of Interconnected Vulnerability etc.

The next day brings the big whopper: the price tag. ILOVEYOU virus costs $10 billion! Really? And how do they arrive at this sum? Any company large enough to rely on e-mail to make its daily bread has on staff a platoon of canny geeks ready to extirpate the offenders and inoculate the system. The problem gets fixed by the guys who are paid to fix problems. Perhaps the techies paid attention to ILOVEYOU instead of other things, and that's where they get the "$10 billion in lost productivity" figure. If so, you could probably say the same thing about the Sports Illustrated swimsuit issue.

. . .

Other articles in this issue also address the topic of viruses and computer security:

- "Campus Computing News"
- "Virus Protection Means Never Having to Say You're Sorry"
- The Network Connection -- "Who do you trust?"
- List of the Month -- "BugNet"

Short Courses

By Claudia Lynch, *Benchmarks Online* Editor

The summer ACS Short Courses will start around June 20. This summer, classes will be taught on "Creating a Homepage with Netscape," and "Creating a Homepage with FrontPage," and there will be training offered on SAS, SPSS, and S-Plus. Please consult the Short Courses page to see if the finalized schedule is available yet.

Customized Short Courses

Faculty members can request customized short courses from ACS, geared to their class needs. Other groups can request special courses also. Contact ACS for more information (ISB 119, 565-4068, lynch@unt.edu).

Especially for Faculty and Staff Members

In addition to the ACS Short Courses, which are available to students, faculty and staff, staff and faculty members can take courses offered through the Human Resources Department, the Center for Distributed Learning, and the UNT Libraries' Multimedia Development Lab.

Center for Distributed Learning

The Center for Distributed Learning offers courses especially for Faculty Members. Topics include those listed in the box below. The center also offers a "Brown Bag" series which meets for lunch the first Thursday of each month at Noon in ISB 204. The purpose of this group is to bring faculty members together to share their experiences with distributed learning. One demonstration will be made at each meeting by a faculty member with experience in distributed learning. Each meeting is followed, for those interested in using WebCT®, by a one hour orientation for beginners in ISB 203. More information on these activities can be found at the Center for Distributed Learning Web site.

Distributed Learning Training - August 2000 Schedule

Attend this four day workshop to become familiar with many aspects of distributed learning, including how to plan for it, course conversion, presentation skills, videoconferencing, and WebCT web course management software. The workshop is offered between long semesters and summer.

Workshop 2: August 14 - 17

See http://www.unt.edu/cdl/training_events/webct_crashcourse_schedule.htm for more information or to register online.

UNT Libraries'

The UNT Libraries' Multimedia Development Lab has also offered free training to all University of North Texas faculty and staff in the basics of FrontPage and information architecture in the past. For more information visit the Multimedia Development Lab's home page at http://www.library.unt.edu/mmdl .

Technical Training

Technical Training for campus network managers is available through the Campus-Wide Networks division of the Computing Center. Some of the seminars, such as one on disaster recovery/business continuity planning techniques, may be of interest to others on campus as well.

UNT Mini-Courses

These are a variety of courses offered, for a fee, to UNT faculty, staff and students. For a free brochure or additional information, call (940) 565-3482 or surf over to http://www.unt.edu/ccecm/cont_ed/index.html for more information.

Alternate Forms of Training

The Training Web site has all sorts of information about alternate forms of training. Training tapes, Computer Based Training (CBT) and Web-based training are some of the alternatives offered.There are also handouts for computer training (Microsoft Office 97 and Windows 95) on the following topics:

- GroupWise 5.2 -- Handout for Win95/NT
- FAQ for GroupWise 5.2
- Info on GroupWise for Win3.1
- Computers - Back to the Basics
- Introduction to Windows 95
- Introduction to Word 97
- Advanced Word 97 - MailMerge It Together
- Introduction to Excel 97
- Introduction to PowerPoint 97
- Introduction to Remedy (THE Call-Tracking Program)
- Using Netscape Communicator and the UNT Home Page

December 1999's "List of the Month" offers links to free Microsoft Word and Excel information also.

Page One

Campus Computing News

Renew PRAS Accounts for the Summer

Need Statistics for Your Website?

Save a Tree. . . E-mail Your Homework!

Virus Protection Means Never Having to Say You're Sorry

HTML Formatting in GroupWise 5.5

GroupWise Document Management: Checking Documents In and Out

RSS Matters

The Network Connection

List of the Month

WWW@UNT.EDU

Short Courses

IRC News

Staff Activities

Subscribe to Benchmarks *Online*

IRC News

Minutes provided by Sue Ellen Richey, Recording Secretary

IRC Regular Voting Members: *Judith Adkison, College of Education; Ginny Anderson, Fiscal Affairs; Donna Asher, Administrative Affairs; Sue Byron, Faculty Senate; Carolyn Cunningham, Student Affairs; Jim Curry, Academic Administration; David Griffiths, Student Association, Don Grose, Libraries; Jenny Jopling, Instruction Program Group; Joneel Harris, Administrative Program Group; Elizabeth Hinkle-Turner, Standards and Cooperation Program Group; Allen Livingston,Graduate Student Council; Dan Mauldin, University Planning Council; Ramu Muthiah, School of Community Services, GALMAC; Jon Nelson, College of Music; Robert Nimocks, Director, Information Technology,UNTHSC; Steve Oeffner, UNT Health Science Center; Russ Pensyl , School of Visual Arts; Patrick Pluscht, Distributed Learning Team; Mark Rorvig, Research Program Group; Paul Schlieve, Communications Program Group; Kathleen Swigger, College of Arts and Sciences; Philip Turner, Associate Vice President of Academic Affairs for Distance Education and Dean of the School of Library and Information Resources (Chair, IRC);; Virginia Wheeless, Chancellor; John Windsor, College of Business.* ***IRC Ex-officio Nonvoting Members:*** *Leslie Bowden, Telecommunications; Jim Curry, Microcomputer Maintenance Shop; Michael Forster, UNT Health Science Center; Richard Harris, Computing Center; Coy Hoggard, Computing Center; Maurice Leatherbury, Computing Center; Sue Ellen Richey, Computing Center (Recording Secretary). [As of 9/99]*

April 18, 2000

VOTING MEMBERS PRESENT: PHILLIP TURNER, CHAIR, SUE BYRON, RAMU MUTHIAH, JOHN WINDSOR, DON GROSE, MARK RORVIG, JONEEL HARRIS, ROBERT NIMOCKS, DONNA ASHER, JON NELSON, CAROLYN CUNNINGHAM, JIM CURRY, PAUL HONS (for JUDITH ADKISON)

NON-VOTING MEMBERS PRESENT: MAURICE LEATHERBURY, COY HOGGARD, SUE ELLEN RICHEY (Recording Secretary)

MEMBERS ABSENT: BILL BUNTAIN, GINNY ANDERSON, ALLEN LIVINGSTON, PAUL SCHLIEVE, STEVE OEFFNER, VIRGINIA WHEELESS, MIKE FORSTER, JUDITH ADKISON, RUSS PENSYL, KATHLEEN SWIGGER, PATRICK PLUSCHT, ELIZABETH HINKLE-TURNER, JENNY JOPLING, LESLIE BOWDEN, RICHARD HARRIS

GUESTS: JENNIFER JOHNSON

The minutes of the March 18, 2000 meeting were not approved, due to a lack of a quorum present. They will be approved at the May meeting.

Distributed Computing Support Management Team

Maurice Leatherbury reported for the Distributed Computing Support Management Team that the committee has continued to work on the campus-wide printer maintenance contract.

Maurice met with Purchasing and they have agreed to draft a request for proposal, which will then be reviewed by a sub-committee of the DCSMT. Maurice explained that he sees this eventual contract as being administered similarly to the campus-wide typewriter maintenance contract; and similarly, departments can buy into it only if they want to. The DCSMT is also evaluating personal digital assistant devices and will provide feedback to the IRC after compiling the results of their findings.

Administrative Program Group

Carolyn Cunningham reported for the Administrative Program Group that Datatel will make a presentation on their mainframe student system to the Program Group, SIMS, AIS group, and any interested IRC members on Thursday of this week. SCT is scheduled for some time in May for their presentation.

Research Program Group

Mark Rorvig reported for the Research Program Group that he has found another NSF program and to prepare for writing a grant proposal is in the process of requesting proposals that have won grants.

Standards & Cooperation Program Group

Maurice Leatherbury reported for the Standards & Cooperation Program Group. He distributed copies of the group's Report on University Computer Inventory and Viability. This report is a result of a compilation of inventory data of UNT departments to determine the numbers and types of computers in use. The report explains the determination of a computer's viability, which is defined as the effectiveness of a machine to fully utilize and run the operating systems and software that reflect the current industry standards for basic computing needs and processes. The purpose of the report is "to accurately and comprehensively supply data for the university community for use (as appropriate) in the planning and implementation of computing resource acquisition and development for the present and future of academic technology." It was explained that the data in the report does not represent machines in labs, and Compaq servers are noted in the "Non-MMS" column. After a short discussion, Maurice noted that each area will have to consider this data in terms of their own needs in order to determine whether or not machines in their area really need to be upgraded.

There being no further business, the meeting was adjourned at 2:30 p.m.

May 9, 2000

VOTING MEMBERS PRESENT: PHILIP TURNER, CHAIR, SUE BYRON, DON GROSE, MARK RORVIG, ROBERT NIMOCKS, DONNA ASHER, JON NELSON, JIM CURRY, JUDITH ADKISON, LOU ANN BRADLEY (for PAUL SCHLIEVE), ELIZABETH HINKLE-TURNER, JENNY JOPLING

NON-VOTING MEMBERS PRESENT: DOWL MORROW (for LESLIE BOWDEN), RICHARD HARRIS, BILL BUNTAIN, MAURICE LEATHERBURY, COY HOGGARD, SUE ELLEN RICHEY (Recording Secretary)

MEMBERS ABSENT: CAROLYN CUNNINGHAM, JONEEL HARRIS, RAMU MUTHIAH, JOHN WINDSOR, GINNY ANDERSON, ALLEN LIVINGSTON, STEVE OEFFNER, VIRGINIA WHEELESS, MIKE FORSTER, RUSS PENSYL, KATHLEEN SWIGGER, PATRICK PLUSCHT

GUESTS: JENNIFER JOHNSON

The minutes of the March 18th and April 18th meetings were approved.

IR Steering Committee

The Chair reported that the IR Steering Committee met and discussed the Report on University Computer Inventory and Viability that was prepared by the Standards & Cooperation Program Group. The report met with mixed reviews, with some concern being expressed that it might be used as a club with department chairs and deans. The vice presidents want the report posted on the web but before doing so wanted to add a statement to the effect that there are a lot of machines currently in use on campus that run just fine at their current levels of software and hardware; although upgrades may be needed in the future. Some discussion followed concerning the two- to three-year equipment replacement cycle.

Distributed Computing Support Management Team

Maurice Leatherbury reported for the Distributed Computing Support Management Team that the group has been working on the renewal of UNT's McAfee software license, determining that it is the package they want to keep for use in virus protection. The DCSMT continues to study personal digital assistant devices and will include the new version of Microsoft's PDA which has been recently released. Maurice also reported the "I Love You virus" incident that was experienced at UNT on May 4th, noting that the DCSMT held an emergency meeting to determine an appropriate response. The GroupWise email system was shut down to prevent the proliferation of the virus; however, all GroupWise post offices were back in operation by Monday morning, May 8th. Network managers had to install the McAfee anti-virus files on all their users' machines. Robert Nimocks commented that since this virus targeted Microsoft, our Novell network and GroupWise were not hit. Once UNT moves to an LDAP system, it will become much more vulnerable to such infections.

Instruction Program Group

Jenny Jopling reported that the Instruction Program Group is meeting electronically, and that she attended the Texas Distance Learning Association meeting where she met with people who are interested in establishing state-wide, computer-based testing. At this meeting, those interested agreed to continue meeting electronically.

Communications Program Group

Lou Ann Bradley reported for the Communications Program Group that at their last meeting they dealt with updates in the wiring plan for Internet I and II, and reported that the long distance contract was awarded to AT&T.

Administration Program Group

Coy Hoggard reported for Joneel Harris that the Administration Program Group, in their continuing efforts to survey available student information systems, hosted Datatel on April 20th. This vendor of student information systems presented a very impressive demonstration; however, at the present time they do not have references from institutions as large as UNT, except for some very large community colleges. Coy announced that SCT is scheduled to make their presentation on Friday, May 12, from 9:00am to Noon in the University Union, Room 418. IRC members are invited to attend this presentation.

Standards & Cooperation Program Group

Elizabeth Hinkle-Turner reported that the Standards & Cooperation Program Group is working on a new project outlining all computing services available at UNT for faculty, staff and students, and attempting to determine who should be and who is eligible for those various computing services.

Video-conference rooms

Dr. Turner announced that the COBA, MUSIC and Physics video-conference rooms are now under construction.

Distributed Learning Team

Jenny Jopling reported for Patrick Pluscht and the Distributed Learning Team that the committee has agreed upon an upgrade schedule for WebCT. An announcement will be made to faculty. They are also planning two classes for faculty in May and September.

Team Web

Maurice Leatherbury reported that Team Web has been meeting to work on a revision of the Web Publishing Policy and Guidelines, because of new state regulations that must be incorporated into those documents. Maurice distributed the draft documents, copies of the existing policy and guidelines, as well as a copy of the new state regulations. There was some discussion of the draft documents and Maurice asked that any comments be forwarded to him prior to the June meeting, at which time, revised documents will be presented for approval by the council.

Jon Nelson moved for adjournment; the motion was seconded, and there being no further business, the meeting was adjourned at 2:40 p.m.

IRC Meeting Schedule

The IRC generally meets on the third Tuesday of each month, from 2-4 p.m., in the Administration Building Board Room. Planned exceptions to this schedule are that December meeting was moved to Dec. 14; that the May meeting was moved to May 9 and the August meeting will be moved to August 8.

All meetings of the IRC, its program groups, and other committees, are open to all faculty, staff, and students.

Staff Activities

Transitions

We welcome the following new employees:

- **Arif Bilgen**, Telecommunications Technical Assistant (part-time).
- **Margaret Ambuehl**, Programmer Analyst on HRMIS team (part-time).

The following people no longer work in the Computing Center:

- **Scott Bryant**, HelpDesk Consultant (part-time).
- **Ramona Aref-Azad**, Production Control Scheduler.
- **Ting-Chun Hang**, Telecommunications Stock Room Clerk (part-time).

Awards, Recognition

- **Rebecca Padia**, Planning and Administration Administrative Assistant, was recognized in the May 2000 Human Resources Newsletter for her suggestion to the TIPS program.
- **Ronnie Seay**, Production Control Specialist, was recognized in the March 2000 *Human Resources Newsletter* as a "Soaring Eagle" for his a"expeditious and professional help setting up an account."

Campus Computing News

By Dr. Maurice Leatherbury, Senior Director of Academic Computing

How do ILOVETHEE(you) -- The virus hits UNT

On Thursday, May 4th the ILOVEYOU virus hit UNT with a vengeance, at least it seemed vengeful for those of us directly affected. If you use GroupWise on campus, and even if you didn't receive the virus, you were still inconvenienced or worse because GroupWise was shut down for the better part of a day or longer, depending upon which department you are in here at UNT. The lessons that were learned from this fast-moving virus were painful, but the following short chronology of what happened to me and others on that day are useful to everyone:*

Thursday, May 4th 8:30 AM	I receive a mail message from a trusted source (the Texas GigaPOP mailing list in Houston), open the message, then click on its attachment. Something starts up that asks me to install Microsoft Outlook, which I don't have on my machine. I declined the invitation.
8:35 AM	My colleague, Coy Hoggard, comes into my office and tells me not to open the message "ILOVEYOU" or its attachment because it apparently does something strange. He had shut his computer down when it seemed to start sending messages without his control.
8:45 AM	Coy and I call our computer support office, which responds immediately and starts investigating what happened. They find that my machine had been infected with the "ILOVEYOU" virus, and start searching on the McAfee virus protection site to find out what that virus does. They learn that it replaces all .jpg, .vbc, and many other file types with some file, and more perniciously, sends the infected message to everyone in your Outlook mail book (note that at least I didn't propagate the virus since I didn't have Outlook installed.) But no virus definition ("fix") file is available yet to protect against ILOVEYOU.
9:15 AM	The Computing Center's virus protection manager, Curry Searle, finds a virus definition file on the McAfee site and downloads it. He starts testing it on his systems but can't verify that it works properly.
10:20 AM	I return from a budget hearing and check to see the status of our efforts to eradicate the virus. I'm told that we still can't get the McAfee fix to work on our systems and that the virus affects even network attached drives. Knowing that some departments still run Web servers whose image files are exposed to the virus, we decide to shut the GroupWise servers down to prevent other users from making the same mistake some of us had already made.
	We still haven't made much progress on getting the McAfee fix

12:15 PM	to work but aren't sure if some of the network managers around campus have. We find at least several hundred messages in the GroupWise system with the subject line of the virus message, so grow more concerned about its spread. We call all network managers to an emergency meeting at 1:30 to discuss the problem and its solutions.
1:30 PM	About 40 network managers and Computing Center support personnel meet, representing all LAN servers on campus. Support personnel from distributed areas report that the instances of actual infections has been low (on the order of ten to fifteen users so far), but that many users had received the ILOVEYOU message. Some network managers reported that they had been able to detect and prevent the virus with the latest McAfee data file, but the fix seemed to be dependent upon the version of the McAfee software as well as having the latest virus definition file installed. There was a lot of disagreement about the seriousness of the threat posed by the virus but the consensus of the group assembled was that we should wait until the campus could find a definitive fix for the virus before turning GroupWise back on.
4:45 PM	The Computing Center's support group for virus protection and LAN services finds a definitive fix to the various versions of the McAfee software on campus that will catch the ILOVEYOU virus before a user opens the attachment. We make the decision to require each network manager to install the fix(es) on their systems before restarting their GroupWise post offices and to let the Computing Center know that they've made the requisite fixes. We call the managers notifying them of this and put it on the Web page with UNT virus information [http://www.unt.edu/virus/].
Friday, May 5th 8:15 AM	The first post office is turned back on after we are notified that all the machines on the post office have been protected with the latest fixes to McAfee VirusScan.
6:00 PM	By the end of the day on Friday, all but two GroupWise post offices have been restarted.
Monday, May 8th 9:30 AM	The last post office is restarted.

What are the lessons that we learned?

There are two aspects of this answer. First, from my own personal experience I learned not to make the following assumptions about e-mail messages:

- Even trusted sources can be the victims of viruses so if you have any reason to question the contents of messages from those sources, beware!
- Virus protection software isn't foolproof, particularly with a fast-spreading infection, so you can't assume that you're protected just because you're using one of the protection packages (the virus "definition" file for ILOVEYOU wasn't available when I was hit.)

- It's absolutely critical that you back up any files that are important to you. I was fortunate in that none of the files that the virus destroyed on my machine or on the network directories was a big loss, but some of our other users did permanently lose files that they needed.

From the campus perspective, we learned:

- We're going to have to be more comprehensive in scanning for file types that may be affected by viruses. Almost no systems on campus were set up to check for Visual Basic scripts, which carried the ILOVEYOU virus. Because of the performance drain imposed by virus scanning packages such as McAfee, most of us only check for the (heretofore) common sources of viruses, the ".com" and Word macro viruses.

- We should attempt to catch viruses before they reach campus, at a single point, so that 6,000 machines don't have to be updated in order to detect and/or prevent viruses. The Computing Center is aggressively investigating solutions that will allow us to do that.

- "Social engineering" (the term coined to explain why many people naively accept messages carrying viruses) can lure even knowledgeable users into launching a virus.

- The campus computing support infrastructure can work quickly and effectively when called upon to do so: we were able to gather over 40 computing support personnel from throughout the campus in less than an hour and to make a decision about the proper course of action.

The ILOVEYOU virus was a costly drain on UNT's time (we measured at least 450 hours of computing support personnel hours alone, costing more than $6,000 in direct costs), but fortunately it did no permanent nor large-scale damage. The lasting message that the virus conveys to us at the University is one from the old Hill Street TV series: "Let's be careful out there!"

Other articles in this issue also address the topic of viruses and computer security:

- "Virus Protection Means Never Having to Say You're Sorry"

- The Network Connection -- "Who do you trust?"

- List of the Month -- "BugNet"

- WWW@UNT.EDU -- "Security on the Internet"

Renew PRAS Accounts for the Summer

By Claudia Lynch, *Benchmarks Online* Editor

If you purchased a **P**remium **R**emote **A**ccess **S**ervice subscription for the spring semester -- or had paid through the spring -- and you want to keep it, you will need to renew it. You may also need to take action to ensure the continuation of your UNT Internet Account, under certain circumstances. Details for renewal of both these services follows.

Premium Remote Access Service Renewals*

Renewals may be purchased in person or over the phone at the software department of the Union Bookstore (940/565 3185). Basic subscriptions for the summer are $30. ISDN (128K) subscriptions cost $60.

These subscription renewals will become active Friday, 2 June 2000. **All subscriptions that have not been renewed by Friday, 2 June 2000 will be deactivated on Monday, 5 June 2000.** Please E-mail any questions regarding renewal to pras@unt.edu

Internet Service Account Renewals

People who are no longer associated with the University lose their eligibility to have access to many services, including various computing services. If you have been notified that your account is going to be disabled and you are still associated with the University, please contact the Computing Center Helpdesk at (940) 565 2324 or to helpdesk@unt.edu. Retirees may continue to have a UNT Internet Service account, however these accounts must be renewed annually. You may be asked to provide documentation of eligibility for this service due to the absence of available data on retirees at this time.

---

*Questions about PRAS? We answered some common ones in our August 1998 PRAS renewal article. The Remote Access area of the Helpdesk Website is also chock full of information on that topic.

Need Statistics for Your Website?

By Shane Jester, Central Web Support

If you have a Website that is hosted by Central Web Support at UNT, you can get a detailed statistical report of Web use for that site. The report will contain a general summary of statistical information including the following:

Successful requests - The number of total successful requests for any files on your site.
Average successful requests per day
Successful requests for pages - the number of total successful requests for Web pages only (does not include images)
Average successful requests for pages per day
Failed requests - number of links to pages or files that do not exist (helps to find invalid URLs in your site.
Redirected requests - any links to built-in redirects on your site.
Distinct files requested - number of different files that were requested through period (duplicate requests not counted)
Distinct hosts served - number of different computers that accessed your site
Data transferred - total amount of data that was transferred in kilobytes
Average data transferred per day

Additionally, you will receive more detailed statistical information including weekly usage breakdown, a list of files requested with the number of requests for each file, and a list of sites that referred your site (i.e. linked to your site).

Currently we produce statistics twice a month. The statistical information periods are the 1st - 15th and 16th - end of month. The statistics are sent via E-mail within a few days of the end of a statistical period. If you would like to receive these statistics please contact jester@unt.edu and include the URL of your Website in addition to the E-mail address where you would like the statistics mailed.

Page One

Campus Computing News

Renew PRAS Accounts for the Summer

Need Statistics for Your Website?

Save a Tree. . . E-Mail Your Homework!

Virus Protection Means Never Having to Say You're Sorry

HTML Formatting in GroupWise 5.5

GroupWise Document Management: Checking Documents In and Out

RSS Matters

The Network Connection

List of the Month

WWW@UNT.EDU

Short Courses

IRC News

Staff Activities

Subscribe to Benchmarks *Online*

Save a Tree.....E-mail Your Homework!

By Dr. Elizabeth Hinkle-Turner, Student Computing Services Manager and Conservationist

Ah, the Paperless University..... *not*! As I lug a huge filled recycle bin from the General Access Lab I manage to the hallway, I pause and think, "Where did we go wrong? Why are so many people printing so many documents? Haven't they heard of turning their papers in on diskette? Shouldn't I really be *working* instead of daydreaming about other people's problems....." As another busy semester ends, it is an excellent time to review printing guidelines and policies in the several UNT General Access Labs scattered around the campus.

Printing Policies for General Access Labs

Printing is a popular past-time in the General Access Labs. After all, what better way to remember the URL of that really cool Metallica Website (you know, the one with all the *pictures*?) than to print out the *entire* site for future reference? In all seriousness, a comprehensive printing policy has been developed for the General Access Labs and is currently published online in the policies and procedures portion of the GAL Website. If you have not reviewed this policy recently, now is the time to do so as it affects all patrons of the labs. Several of the labs also have more detailed policies, and it is important for faculty, staff, and students to be aware of these when assigning and/or completing schoolwork and other tasks. **Only work which falls under the university guidelines for meeting the degree requirements for all courses taken may be printed in the General Access Labs, and printing will be provided only to UNT students as it directly relates to their class work.** Printing activity generally revolves around Internet class work and research; the creation of assignments and papers; the development of flyers, posters, and artwork; and the final printing of important large-scale projects and reports. **The lab manager has the final authority in all printing policies and procedures for his or her lab.**

Internet printing for courses is not permitted unless the lab manager is made aware of and has also approved of the nature of the print job. Most Internet

content does not need to be printed; students can take notes from the digital page as easily as they do from other research texts. Additionally, with the increased opportunity to take courses online, students and faculty alike should plan for a minimum amount of necessary printing for these classes. **All lab users are responsible for knowing how many pages an Internet document contains before they execute a print job**. Several of the General Access Labs have color printing but few allow the printing of Web pages in color. Class notes, course instructions, and Web- and multimedia-based materials should not be printed in the labs. Course instructors should print these materials using departmental resources and hand them out in class. Email also should not be printed and if PowerPoint presentations must be printed, several "slides" should be included on each page. (the printing of PowerPoint presentations is strongly discouraged and is also unnecessary as these can easily be saved onto disk.)

The printing of assignments and papers is welcome in the labs but more than 20 pages of printing per job is not allowed. Additionally, if copies of documents are being printed for revision, please be sure to utilize the toner-saving draft copy settings. Users are also encouraged to employ double-sided printing when at all possible. Ask a lab monitor if "duplexed printing" is available and have them demonstrate how to set options for double-sided work if needed. Please notify the lab manager about the printing of large jobs like a thesis or dissertation. These large print jobs should be scheduled for execution during off-peak hours, evenings, or weekends. Finally, the multiple copying of a document is not permitted. Most areas have Xerox machines and people needing extra copies can print them on these.

Several labs on campus have special printing services available in them for patrons creating artistic content such as flyers, graphic designs, and signs. Lab users are not allowed to print such items unless they are directly related to UNT course work and proof of this is required. Labs with color printing and large-scale printing usually have specific restrictions for these services, and users should check with each lab's manager about these policies. Many of the labs also have their regulations posted and available on the Web for easy access.

Finally, **lab managers have the authority to grant special printing requests and to specifically *deny* printing and lab access for any user who abuses printing policies.** Lab managers meet regularly to discuss and review the printing needs of General Access Lab users and to keep up to date on the abuse of policies already in place. **The University of North Texas is one of the few institutions to have free laser printing available to its faculty, staff, and students, however, abuse of this rare privilege could lead to the establishment of additional printing fees in the future.**

In the meantime, all campus computer users are encouraged to "turn over a new leaf" (and save one in the process!) and trying living digitally. Ask professors if they will accept emailed papers instead of hard copies, save favorite Web pages and URLs to disk, and take notes and info from the Internet like you would from a "physical" text in the library. The tree you save might be your own (you know, that scrawny one in your front yard.....) !

Save a Tree.....E-mail Your Homework!

Virus Protection Means Never Having to Say You're Sorry

By Claudia Lynch, Benchmarks Online Editor

Protecting your computer from viruses just might mean never having to say you're sorry. A lot of people around the world were hit with the ILOVEYOU virus recently, but a lot more weren't because they quickly inoculated their PCs with the latest virus protection files (or someone did it for them).* It is **VERY** important to make sure you have viral protection software running on the computers that you use, both at home and at work.

Here at UNT the Network Managers are generally responsible for keeping the people in their departments informed about such things, but if you're unsure about the status of such software on your computer, you probably ought to contact your Network Manager and ask. If you're not sure who your Network Manager is, check here http://www.unt.edu/helpdesk/netman.htm.

Curry Searle, the Computing Center's virus protection manager, recently re-vamped the UNT Anti-Virus Resources page (http://www.unt.edu/virus/). This site is accessible to anyone on campus or who comes into campus via the UNT dial-up lines. If you satisfy those requirements, the anti-viral software is available to you from there free-of-charge.Once you have the software it is wise to set it to run every time your computer is re-started (you can always cancel it if you have to re-start several times). You should also set it to automatically update.

Automated VirusScan Updates

Wil Clark, who used to be the campus virus guru, wrote an article on "Automated VirusScan Updates" last October. Here is an edited version of Wil's instructions for setting VirusScan to automatically update:

> Remember these features are discussed here primarily to help you with your **home computer**. You should check with your network administrator before making any changes to your UNT computer as your administrator may have a different mechanism in place for updating it.
>
> You will need to have McAfee VirusScan installed on your computer to use these features. UNT students and employees can download a copy of McAfee VirusScan from http://www.unt.edu/virus/. Please note that you must be on the UNT network or connected through UNT's dial-up access to download these files.
>
> We will configure VirusScan to update its virus definition (dat) files. You may recall that this is the information that VirusScan uses to identify viruses. McAfee releases new datfiles weekly. We will use McAfee VirusScan Scheduler. Perform the following steps:

1. Launch McAfee VirusScan Scheduler (Start -> Programs -> McAfee VirusScan -> McAfee VirusScan Scheduler).
2. Open AutoUpdate properties (Right-click on AutoUpdate then click on Properties).
3. Click Configure… button.
4. Delete existing Update sites (Click on a site then click Delete button; repeat for each site).
5. Add UNT update site (Click Add… button).
6. Type UNT for Site Name.
7. Enable site (click on and ensure a check mark appears in the Enabled box).
8. Choose FTP for Select Transfer Method (click on and ensure a dot appears in the FTP circle).
9. Type **ftp.unt.edu/pub/antivirus/datfiles/4.x** for the FTP computer name and directory field.
10. Enable Anonymous FTP Login (click on and ensure and check mark appears in the Use anonymous FTP login box).
11. Click OK on the Automatic Update Properties dialog box.
12. Click OK on the Automatic Update dialog box.
13. Click the Schedule tab on the Task Properties dialog box.
14. Enable the automatic update (click on and ensure a check mark appears in the Enable box).
15. Choose a frequency for the update to run (click on one of the choices in the Run section). Note: your computer must be on and connected to the Internet for this to work. It might be useful to choose a more frequent update period to ensure that you get weekly updates.
16. Choose an appropriate Start at time for the frequency you selected.

Once this is configured your computer will automatically look for updates to the Datfiles. Your virus scanning software will be updated and you don't have to remember to update it. Each time your dat files are updated. you will be prompted to reboot your computer. This must occur to begin using the new dat files.

Crispen's Six Antivirus Rules

Now that we've got that out of the way, we've satisfied rules #1 and #2 of "Crispen's Six Antivirus Rules." Patrick Douglas Crispen is the author of the Internet TOURBUS. In the Volume 5, Number 89 -- 4 May 2000 issue, Patrick rewrote his virus protection rules. If you follow them you really may never have to say you're sorry, at least about losing data/crashing your computer due to a virus.

Crispen's *SIX* Antivirus Rules -- 4 May 2000

In light of the recent "ILoveYou" worm outbreak, I decided to re-rewrite my rules on how to protect yourself from computer viruses, Trojan horses, or worms. Regardless of your operating system, these six rules should protect you from most of the over FORTY-SIX THOUSAND viruses that are currently floating around the Net (including the "ILoveYou" worm).

1. PURCHASE A GOOD, COMMERCIAL ANTIVIRUS PROGRAM

LIKE NORTON ANTIVIRUS OR MCAFEE VIRUSSCAN.

Most commercial antivirus programs usually cost between US$40 and US$50 and can be purchased at almost any computer store in the world. [You can usually save about US$10 if you purchase the software online -- visit http://www.shopper.com/ for more information].

Antivirus program manufacturers also release minor upgrades every two to three months and major upgrades every twelve to eighteen months. YOU NEED THESE UPGRADES. Minor upgrades are usually free, and major upgrades usually cost anywhere between US$20 and US$40, depending on the manufacturer [think of this as an expected expense -- just as you have to change your car's oil every 3,000 miles, you have to upgrade your antivirus software every year to year-and-a-half].

To see if any minor or major upgrades are available for your antivirus program, visit your antivirus program manufacturer's homepage. A list of antivirus manufacturers' homepages can be found at http://www.yahoo.com/ or at AOL keyword "virus."

2. UPDATE YOUR VIRUS DEFINITIONS FREQUENTLY (AT LEAST ONCE A WEEK).

With over 250 new viruses being discovered each week, if you don't update your definitions frequently you won't be protected from ANY of the new viruses floating around the Net.

How do you update your virus definitions? That depends on the antivirus program you use. Norton Antivirus has a "Live Update" button built into the program; click on it, and Norton automatically downloads and installs the latest virus definitions from Net. McAfee VirusScan has a similar update function (go to File --> Update VirusScan).

If you are unsure of how to update your virus definitions, visit the homepage of your antivirus software manufacturer and look for their "download," "update," or "technical support" section.

3. NEVER DOUBLE-CLICK (OR LAUNCH) *ANY* FILE, ESPECIALLY AN EMAIL ATTACHMENT, REGARDLESS OF WHO THE FILE IS FROM, UNTIL YOU FIRST SCAN THAT FILE WITH YOUR ANTIVIRUS PROGRAM.

This is probably the most important rule of them all. There are currently over forty-six thousand viruses out there, there are over 2.8 trillion possible files names out there, and any one of those viruses could be hiding in any one of those file names. A lot of people think that you can protect yourself from a computer virus by being on the lookout for one particular virus or one particular file name (hence all of the virus warnings you have received in your email inbox lately).That's not only silly, that's dangerous. If you want to protect your computer from viruses, you need to ignore ALL of the virus warnings you receive and instead beware of EVERY file you see, especially every file that is attached to an email message.

It is important to note that, despite all of the warnings to the contrary, there is no such thing as an email virus. If you are running the most up-to-date version of Windows (see rule #5 below) or if you have a Mac, you can open your emails, regardless of their subject lines, without fear of infecting your computer, provided your email program doesn't automatically open attachments (most don't). It is the files that are ATTACHED to emails that you have to fear.

Think of a computer virus as a well-packaged letter bomb. You can move a letter bomb from room to room in your house without any danger. Open the letter bomb, however, and you die. The same is true with computer viruses. You could download a billion virus-infected files from the Internet and receive another billion virus-infected files attached to email messages and your computer still wouldn't be infected with a virus. Open, or double-click on, just ONE of those files, though, and your computer is dead.

Remember, to infect your computer with a virus, you have to open (or double-click on) a file that contains a virus. As long as you don't open that file, you really have nothing to fear.

How can you scan a file for viruses? That depends on the antivirus program you use. The best bet is to read your antivirus program's instructions or read its online help section. If you use Norton Antivirus or McAfee VirusScan, right-click (or, if you have a Mac, click and hold) on the file in question. A pop-up menu should appear, and one of the choices should be "Scan with ..." and the name of your antivirus program. If that doesn't work, just open your antivirus program and try to scan the file from there.

Do you have to scan EVERY file, even if that file is from your friends or coworkers? Yes! The Melissa, WormExplore.Zip, and "ILoveYou" viruses distributed themselves by opening your email program, looking at either your 'friends' list or the list of email addresses in your inbox, and then distributing virus-infected files to everyone on that list.

In the world of computer viruses, you can't trust ANYONE (even if they say they love you). :P

4. TURN ON MACRO VIRUS PROTECTION IN MICROSOFT WORD, AND BEWARE OF ALL WORD MACROS, ESPECIALLY IF YOU DON'T KNOW WHAT MACROS ARE.

Word Macros are saved sequences of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke. They enable advanced Word users to easily accomplish what would otherwise be difficult tasks.They also allow virus writers to do serious damage to your computer. For example, the Melissa virus was actually a Word Macro virus.

If you use Word 97, go to Tools --> Options. Click on the "General" tab. Make sure that "Macro virus protection" (at the bottom of the list) is checked.

If you use Word 2000, Double-click on the Tools menu, point to "Macro," and then choose "Security." Select the level of security you want. High security will allow only macros that
have been signed to open. Unsigned macros will be automatically disabled. Medium security always brings up the macro dialog protection box that allows you to disable macros if you are unsure of the macros.

With Macro virus protection turned on, Microsoft Word will warn you every time you try to open a Word document that contains a macro. The warning gives you three choices: the option to open the file but disable its macros ("disable macros"), open the file with macros enabled ("enable macros"), or the option to not open the file ("do no open"). Chose the first (default) option: "disable macros."

For more information, visit the Macro Virus Protection page at http://officeupdate.microsoft.com/focus/articles/o97mcrod.htm

5. RUN WINDOWS UPDATE AT LEAST ONCE A MONTH

Windows is aptly named because it is full of holes. There are several, inadvertent 'open doors' (or 'security holes') in the Windows operating system that *COULD* conceivably make your computer vulnerable to outside attack. In specific, a mean-spirited hacker *COULD* 'walk through' one of these open doors on your Windows PC and read any file on your computer, delete specific files or programs, or even completely erase your hard drive.

When the folks at Microsoft discover a security hole, they immediately release a software patch to close it. Without the patch -- and there are MANY -- your computer is wide open to outside attack.

Fortunately, downloading these patches couldn't be simpler.Built into every 98 PC (and into every version of Microsoft's Internet Explorer since version 4.0)is something called"Windows Update." Windows Update is an easy-to-use tool that helps you ensure that your PC is running the absolute latest Microsoft software patches and drivers.

Here is how to use Windows Update to download all of the security patches Microsoft has released since your PC was made:

1. Connect (or logon) to the Internet.

2. If you have Windows 98, launch Windows Update by going to Start --> Settings --> Windows Update on your PC. You can also launch Windows Update by going to Tools --> Windows Update in either Internet Explorer 4 or 5. Either way will connect you to Microsoft's Windows Update page [http://windowsupdate.microsoft.com/].

By the way, if you don't have Internet Explorer 4 or later, Microsoft's Windows Update page will automatically talk you through the process of downloading and installing the latest version of Internet Explorer.

3. On the top left-hand side of the Windows Update page, click on the "Product Updates" link (it is the one with the hand and the red *)

4. A pop-up window will appear, telling you to wait while your computer DOESN'T send any information to Microsoft (well, that's what it says!)

5. Eventually, you'll see a page that says "Select Software." When Microsoft releases an essential update or patch to close a security hole in Windows, they put it in this page's "Critical Updates" section. Select (or click on) EVERYTHING in the "Critical Updates" section -- you need *ALL* of the critical updates -- and then click on the big, gray "Download" arrow in the top right hand corner of the page.

6. Follow the on-screen prompts. That's it! :)

New security holes are found in Windows every week or two, so it is a good idea to run Windows Update at least once a month. The first time you run it, expect to see a MESS of critical updates. After that, though, there should only be one or two critical updates you'll have to download every month.

6. IF SOMEONE UNEXPECTEDLY SENDS YOU AN EXECUTABLE FILE OR VISUAL BASIC SCRIPT FILE -- IN OTHER WORDS, A FILE THAT ENDS IN .EXE OR .VBS -- THROW IT OUT.

Most of the forty-six thousand viruses that are floating around the Net right now are hiding in executable files. Some of the most vicious, new viruses are hiding in Visual Basic script files. If someone, even a close personal friend, unexpectedly sends you a file that ends in .exe or .vbs -- or if they unexpectedly send you a zipped file that contains a file or files that end in .exe or .vbs -- your safest bet is to delete the file without opening it.

The key word here is "unexpectedly." If you are expecting a friend to send you an executable file, you certainly don't need to delete that file -- just virus scan it first before you open it.

However, if you are in an environment (like a home) where you don't often receive ANY files attached to your incoming email messages, a better rule would be: "When in doubt, throw it out... and doubt EVERYTHING."

How well will these six rules protect your computer from becoming infected with a virus, Trojan horse, or worm? Take a look at the following questions, and decide for yourself. How many people whose computers were infected with the "ILoveYou" virus ignored at least one of these rules? ALL OF THEM! How many people who followed these six rules had their computers infected by "ILoveYou?" NONE OF THEM! How many people whose computers were infected with the WormExplore.Zip virus ignored at least one of these rules? ALL OF THEM! How many people who followed these six rules had their computers infected by the WormExplore.Zip virus? NONE OF THEM!

These six rules will not protect you from every computer virus, Trojan horse, or worm, but they will so significantly decrease your computer's

chances of becoming infected that you can all but forget about the next virus scare and all the ones that will follow.

---

*Of course if you were using a Mac or weren't running the Windows Operating Environment, you couldn't have gotten the virus anyway, it was/is Windows-based.

Other articles in this issue also address the topic of viruses and computer security:

- "Campus Computing News"
- The Network Connection -- "Who do you trust?"
- List of the Month -- "BugNet"
- WWW@UNT.EDU -- "Security on the Internet"

HTML Formatting in GroupWise 5.5

By Mike Williams, Campus Wide Networks Desktop Support Specialist

Are you aware of the HTML formatting capability of the GroupWise 5.5 Enhanced Client?

- You can add images in gif, jpg and bmp format to your messages.
- You can ***format your text*** using different colors and fonts with bold, underline and Italics.
- You can add an image to the background or pick a background color.
- You can add horizontal lines.

To use the HTML formatting in GroupWise you will need to create a new mail message (click on FILE>NEW>MAIL or press Control + M). Then click on VIEW>HTML. Now you will need to open the message full screen to see all the toolbar icons on the bar above the body of your message. Just move your cursor over the toolbar icons to get a toolbar message telling you what function each icon has. Important: When adding an image to an email you must deselect the image before you send the message or it will cause problems and shut down GroupWise. To make sure the image is deselected click on it and then click somewhere else in the body of the message, the resize boxes should be gone from your image. Just experiment and have fun sending cool E-mail.

More Information

For more information about the GroupWise 5.5 Enhanced Client, drop by http://www.unt.edu/cwn/gw55cbt/index.html and take the GroupWise 5.5 Enhanced Client CBT tour.

GroupWise Document Management: Checking Documents In and Out

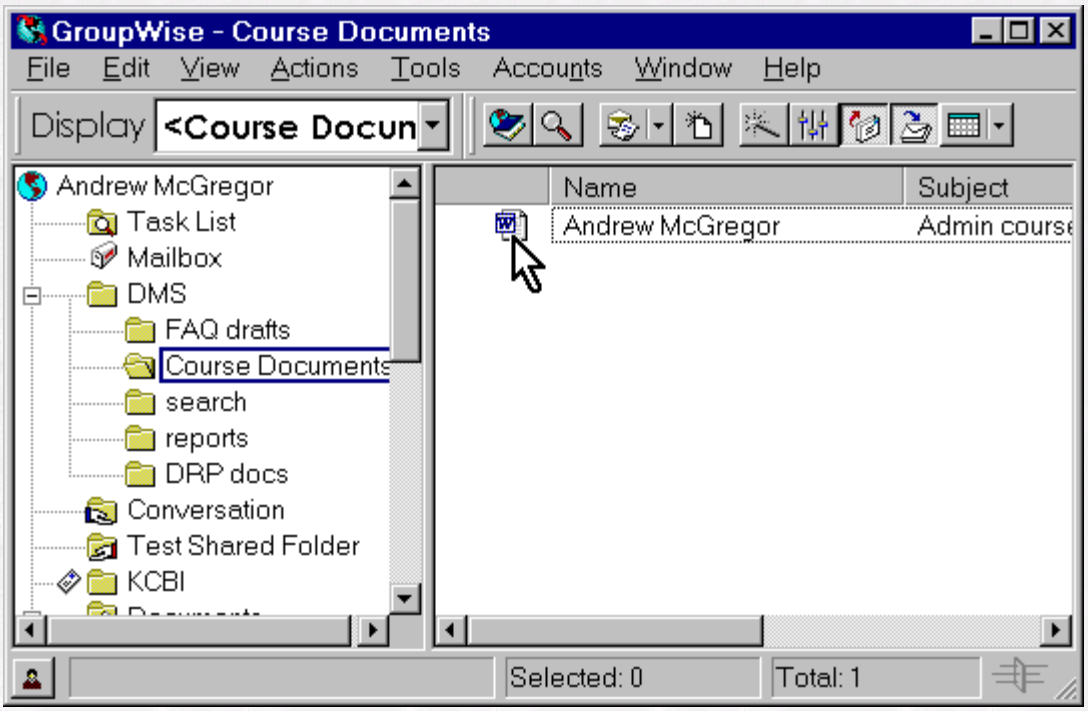
This is the fourth in a series of articles on the topic of GroupWise Document Management. This article does not deal specifically with the GroupWise Macintosh Client, which will be covered at a later date.

By Andrew McGregor, Messaging Support Specialist

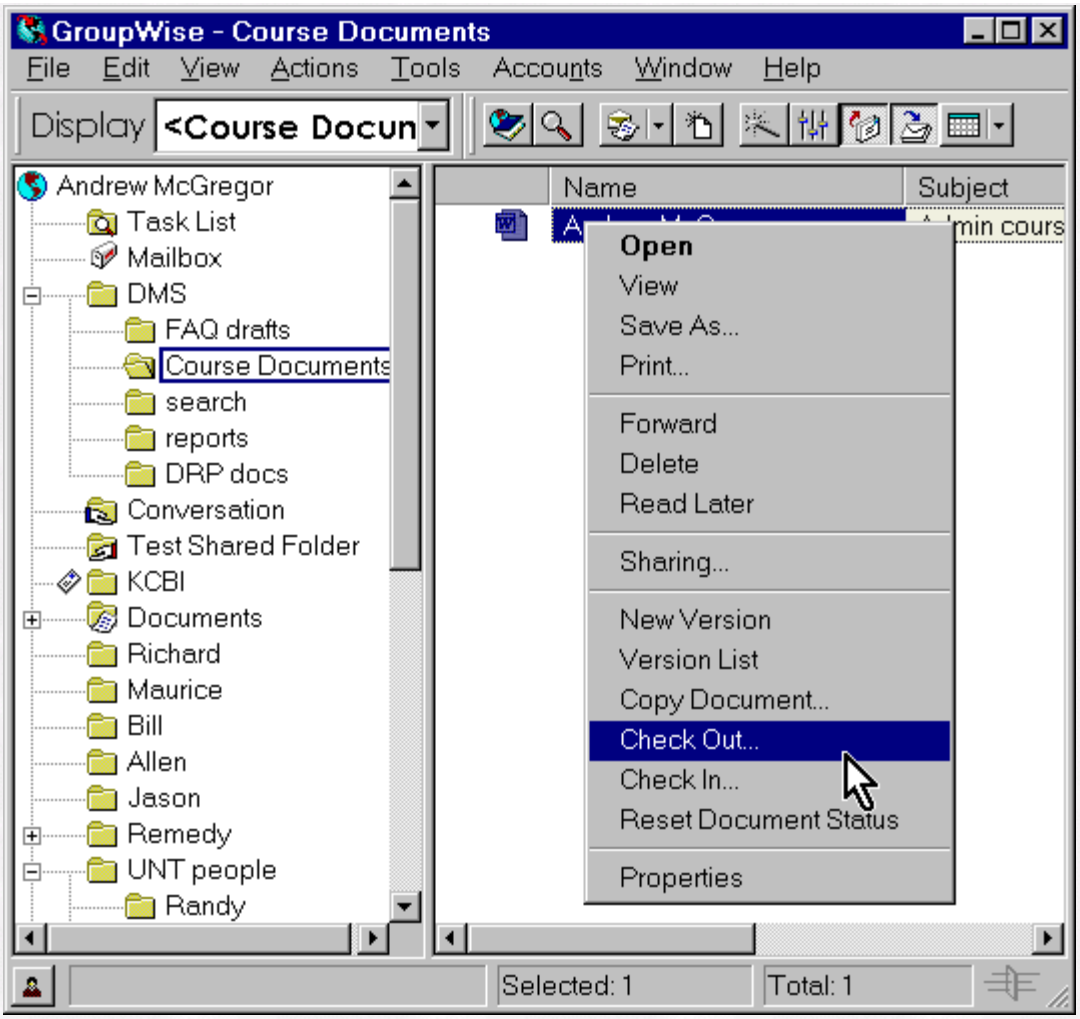
One of the neat features of the GWDMS is the ability to check documents out. In some situations, you may have several people working on a single document at the same time. But you may want to edit the document yourself, and "lock" the other users out. Although opening the document "locks" users out, it only does so while you have it open. When you check a document out, it becomes inaccessible to the other users until you check the document in. In this way, you don't have to leave the document open in order to "lock" the document.

Checking Documents Out

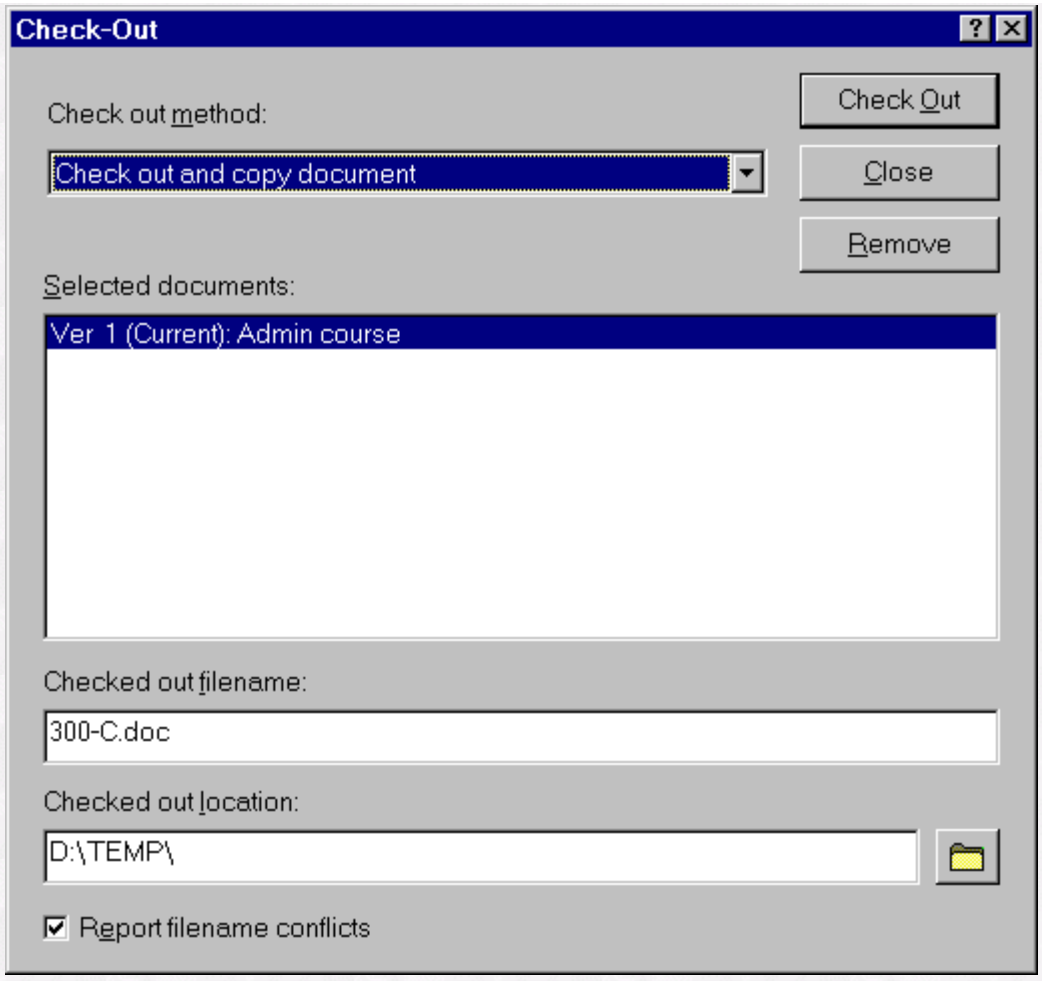
Let's look at how this is done. Start off by selecting a document to check out.



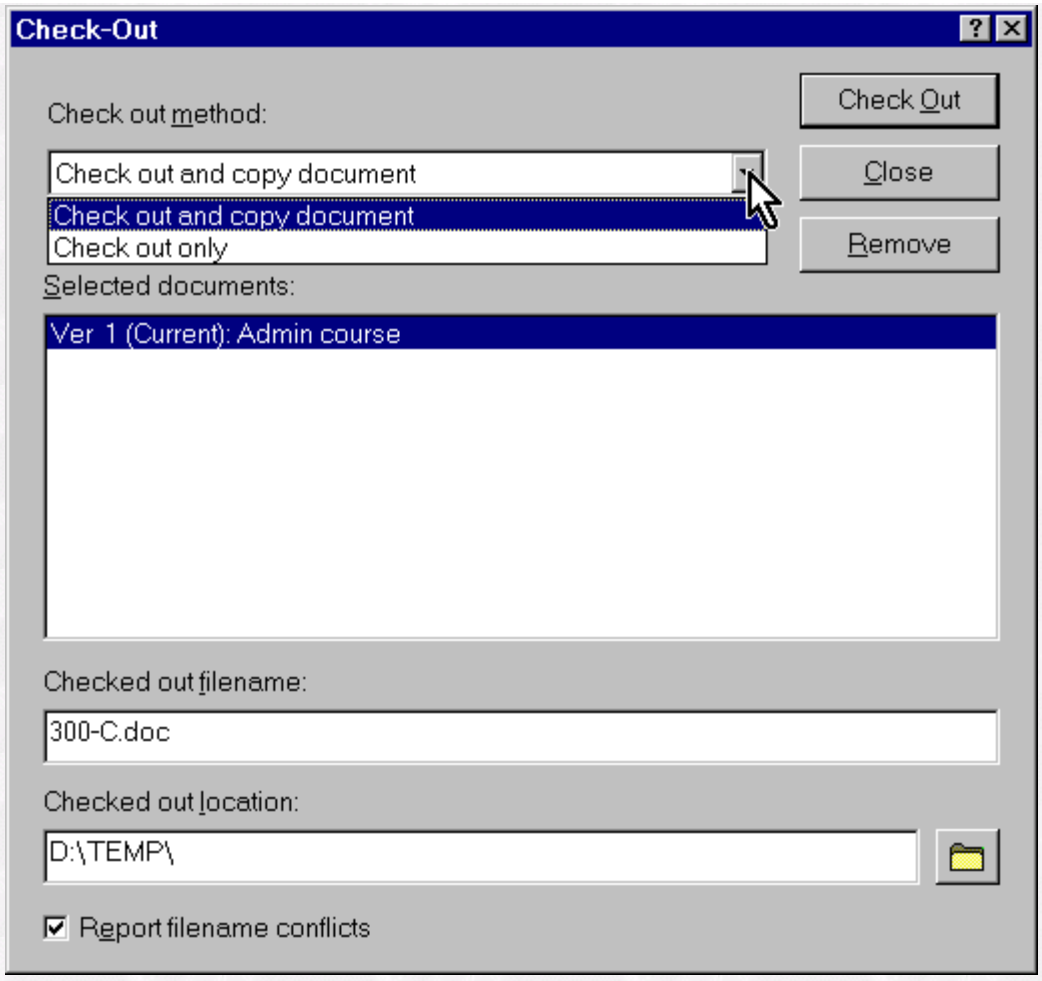
There are a couple of ways to get to the next part. The first way is to "right click" on the document and choose "Check out…". The next way is to click on "Actions" in the main menu bar, and choose "Check out…". We'll look at the "right click" method in this section.



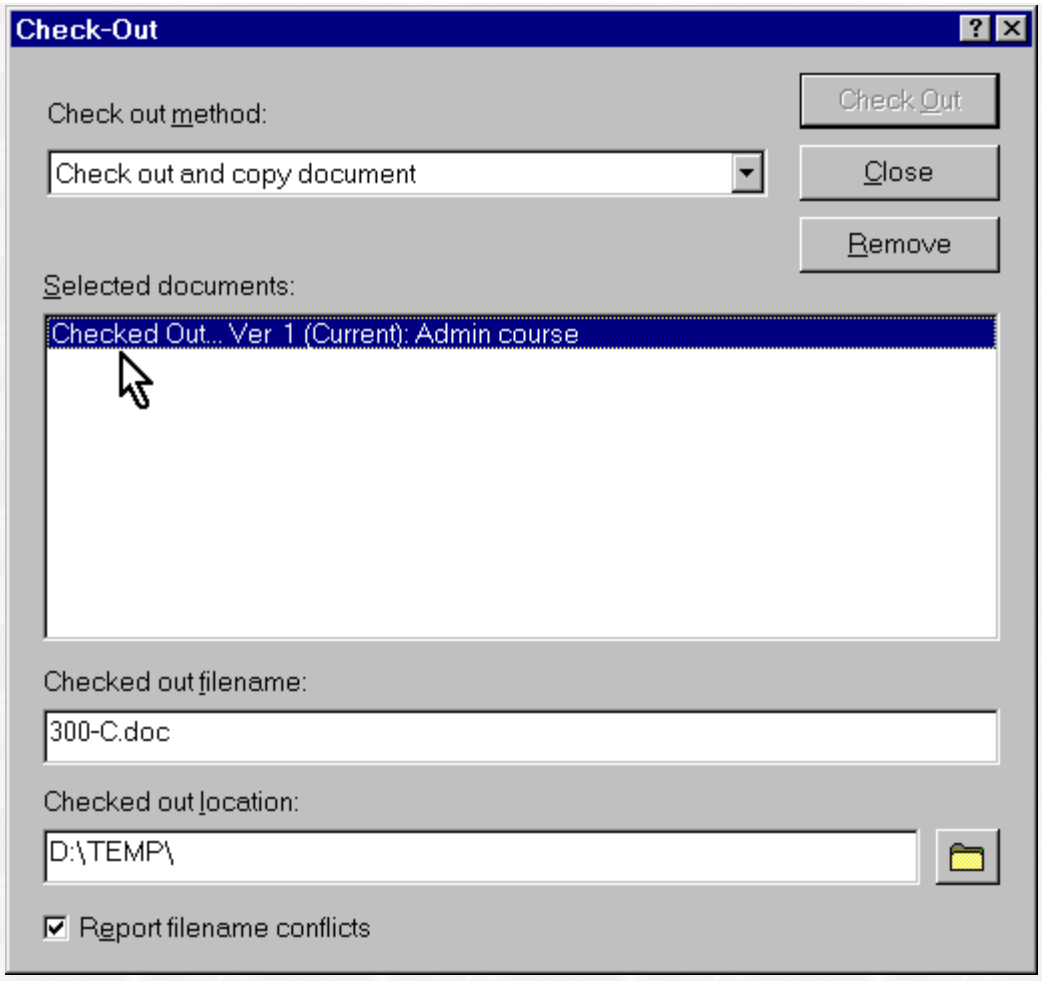
After clicking on “Check out…”, you’ll see the screen below.



In the “Check-Out” screen, you’re given two options for check out. “Check out and copy document” means that the document will be checked out and a copy of it will be placed in a location of your choosing. “Check out only” means that the document will be inaccessible to everyone including you. So, if you want to work on the document while it’s checked out, I suggest you choose the first option. Below the "selected documents" window, there are two fields. The first one is for the file name. You can use the default name, or change it to whatever you would like. The second field is for the path to the folder where the document will be saved. As with the name, you can use the default or choose where you want the document to go. If you are satisfied with your choices, click on the “Check Out” button.

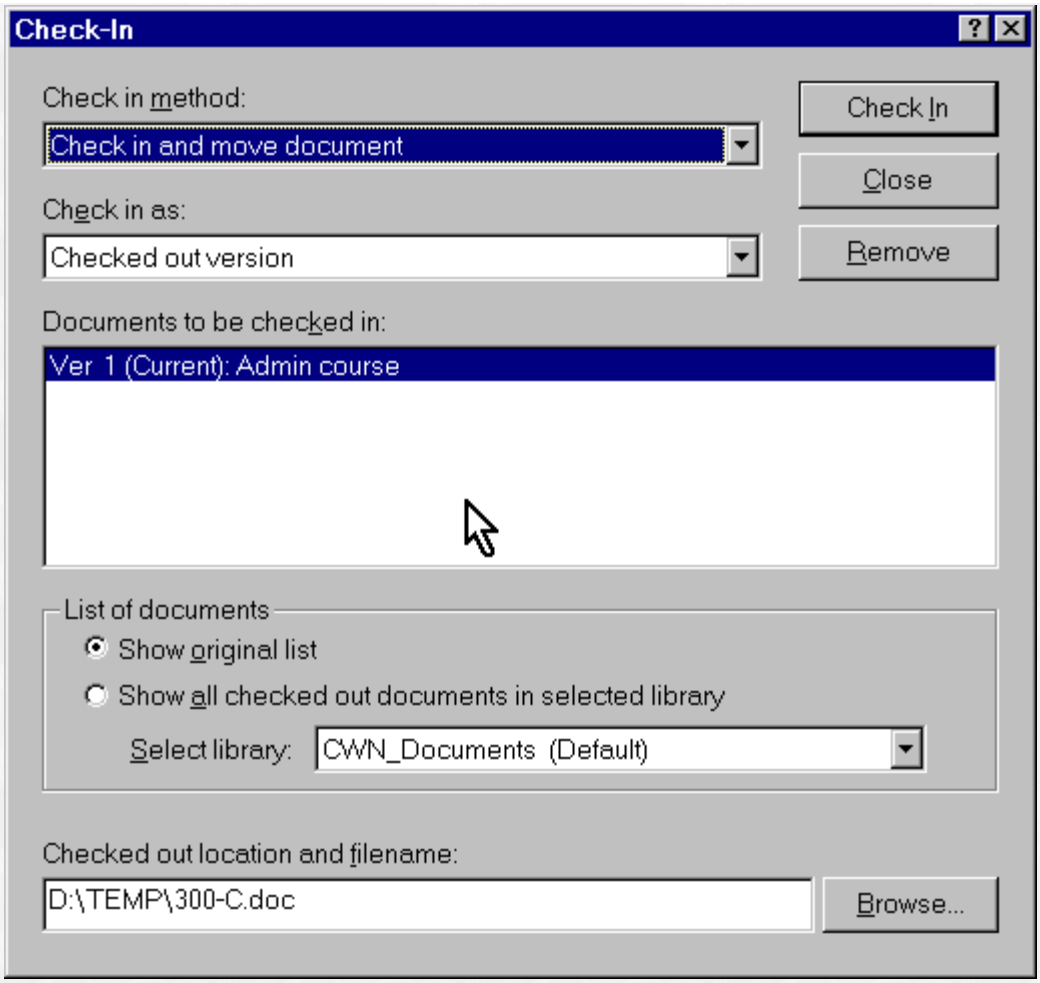


When the document has been checked out you will see the text in the “Selected documents” window change, and reflect, “Checked out…”. At this point, you know the document has been checked out. Now, you should have a document in the folder that you chose that you could open and edit, but no one in the GroupWise system can edit it.



Checking Documents In

Checking a document in is just as easy as checking one out. The first thing you will need to do is select the document reference of the document you want to check in. Then “right click” on it and choose “Check In…”. This will bring up the “Check-In” window. The “Check In” window has a number of options that we will look at. First, we will look at the “Check in method:” window.



There are four options for the “Check in method:” field. I will explain each.

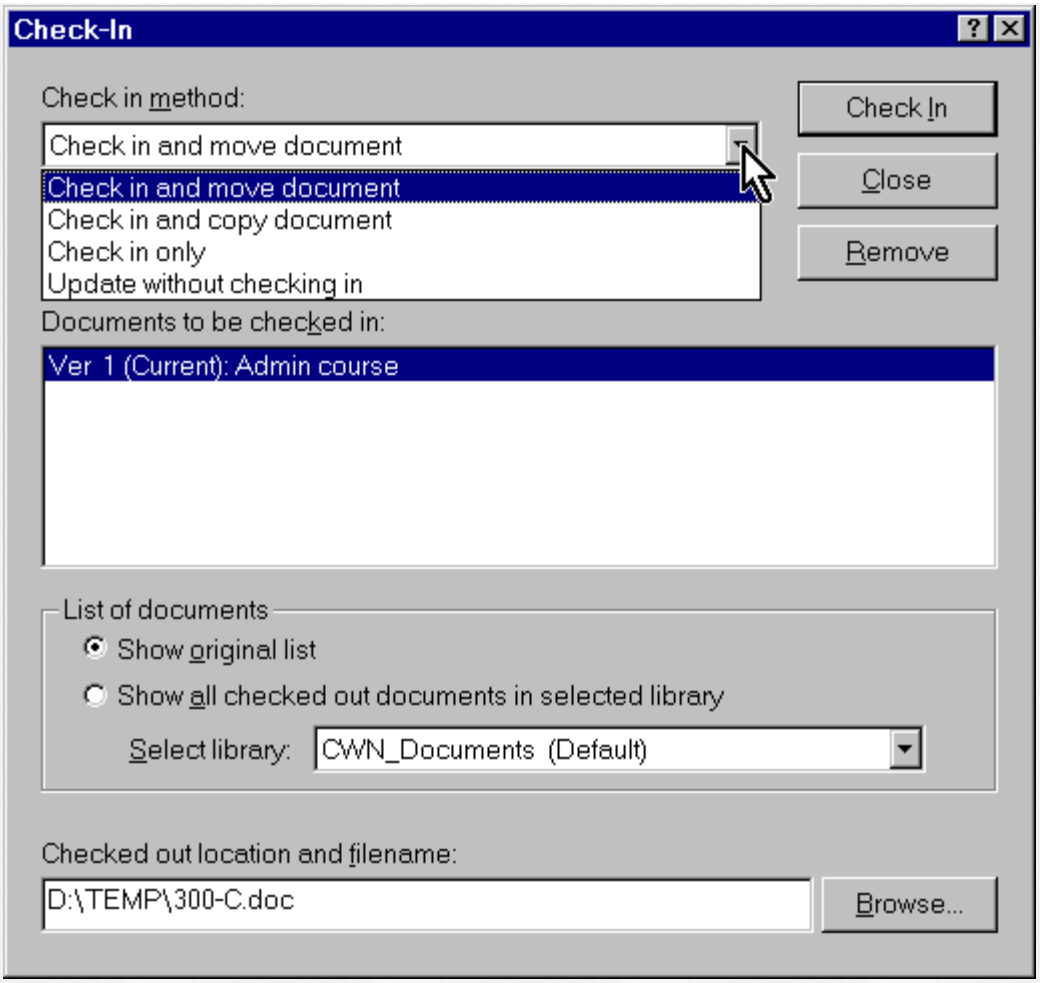
1. **Check in and move document**– If you chose “Check out and copy document” when you checked the document out, this option will update the document in the library with the changes, delete the copy, and unlock the document in the library. If you chose “Check out only”, this option won’t work, because it needs a valid file path to update from.

2. **Check in and copy document** – This is the same process as the first one except the copy is not deleted.

3. **Check in only** – This option unlocks the document and does nothing else. No changes get made to the document in the library.

4. **Update without checking in** – This option is used when you have a copy of a document made and you want to update the document in the library without making the document available for other users to edit.

So make your choice of how you want it checked in and then we will look at the next window.



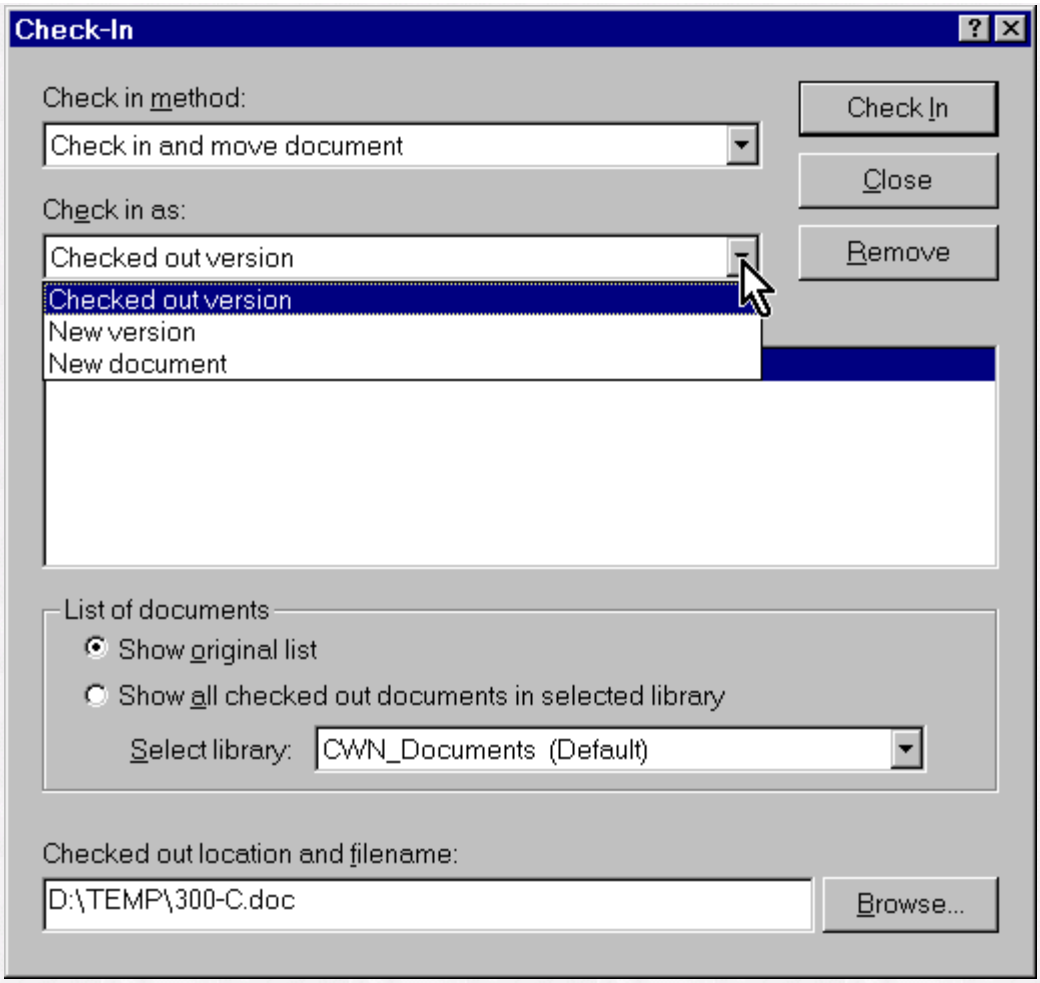
The “Check in as:” field has three options to choose from. Here is an explanation.

1. **Checked out version** - If you made changes to a document and just wish to update the document you checked out, you need to choose this option. This will leave the document as the original version.

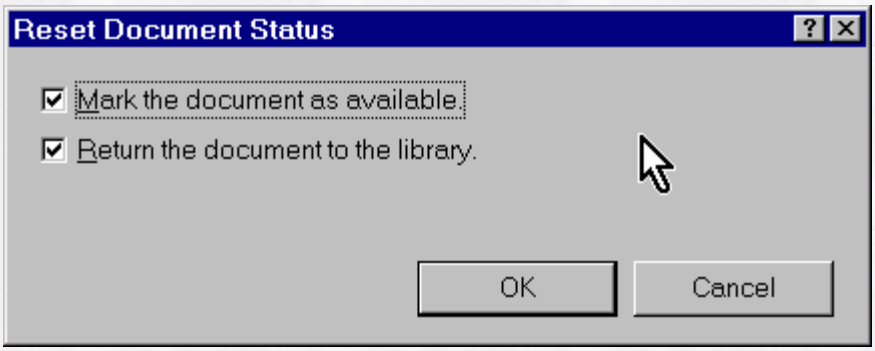
2. **New version** - If you made changes to a document and would like to use the changes to form a second version of the document, then choose this option. This will use the updated version of the document that you are checking in to create a new version.

3. **New document** - If you don’t want to update the original version and you don’t want to create another version, then you will want to create a whole new document. If this is the case, you need to choose “New document”.

After you have decided which option to choose, go ahead and click “Check In”. Poof, your document is checked in.



Sometimes when checking in a document, you may want to open that document quickly thereafter. When doing this, you may get a message saying that the document is not available or that someone has it opened or checked out even though you know it's checked in and not being used. What you need to do is reset the document's status. You do this by "right clicking" on the document reference and choosing " Reset Document Status". The screen below will appear. Sometimes the document is not properly returned to the library or it hasn't been "unlocked" yet, which would cause you to not be able to open the document, so putting a check mark in the two boxes and choosing "OK" should normally take care of the issue.



More Information

Stay tuned for more neat GroupWise Document Management features next time. If you want to do some reading in the meantime, check out the topic of "Document Management" in the Novell GroupWise Cool Solutions vault.