

June 2001
Vol. 6 No. 2

Do you qualify
for automatic
virus checking
of your email
enclosures?1

Is big brother
watching you
in the library?3

Have you checked
out the summer
savings from
TechMart?10



Need training?

Look for the summer
computer short
course schedule on
the University
Technology Training
Center's Website:

training.micro.umn.edu/ShortCourses/



Information Technology

Newsletter

Automatic Virus Checks

A new Office of Information Technology service for TC central email accounts

TC central inboxes are scanned

The Office of Information Technology (OIT) has good news. All email delivered to *central Twin Cities* email accounts is now scanned for viruses. This virus scanning includes .ZIP and other compression file types. So if you are using

`internetid.email.umn.edu`

• *for example: larse789.email.umn.edu — where larse789 is the internetid*

as your mail server, then email delivered to your inbox (incoming mail server) will be checked for viruses. (POP and IMAP protocols are supported.) Mail in which no suspicious “virus signatures” are detected is delivered exactly as sent, preserving the email’s integrity for digital signatures, etc. Since the majority of email that people receive is delivered exactly as it was sent, the email has no indication that virus scanning took place.

If a virus is suspected

However, if a suspicious virus signature is found, the following message will be added to the beginning of the email that contains the suspect “signature.”

```
Warning!! A possible virus has been detected in your message.  
The name of the virus is given below:
```

```
Virus Name: [**name**]
```

```
We strongly recommend against opening attachments to this letter  
unless you understand the risks involved.
```

A message is also sent to the originator of the message if a virus is detected. Because virus detection takes place immediately prior to final delivery of a message, originators can receive multiple copies of the warning, due to the fact that people on their recipient list are typically using different mail servers. The message the originator of the message will receive is:

```
A possible virus (["**name**"]) was
detected in the message you sent to:
```

```
[internetid@UMN.EDU]
```

```
This indicates that your computer may
be infected with the virus, or that
you have forwarded an infected file.
You should examine your options to
clean your computer of the potential
virus infection.
```

Other inboxes

If you use your Twin Cities centrally assigned inbox, then your incoming email is automatically scanned for viruses. Mail gets delivered to that inbox when you use **internetid.email.umn.edu** as your incoming mail server. This service is available to all current students, faculty and staff.

Some people don't use internetid.email.umn.edu as their inbox for some or all of their email. They may maintain multiple inboxes or have email addressed to their centrally assigned TC email address automatically forwarded (sent) to a different email server — such as a departmentally maintained server or AOL's mail server.

These other mail servers may or may not automatically scan for viruses. OIT only scans mail delivered to internetid.email.umn.edu inboxes for viruses, and it scans that mail regardless of its origin.

Infection rate

Since installing virus detection software, the rate at which infected emails have been detected has varied between 0.1% and 0.5% of all email processed.

In a typical week we will process approximately 3,000,000 emails. (Note: email with multiple recipients is counted as one message). This translates to between 3,000 to 15,000 messages containing viruses per week!

Virus Signatures

One tactic of antivirus software is to look for patterns in computer code that are like the patterns found in known viruses or other malware (malicious software); these patterns are known as signatures.

Virus signatures are updated automatically when the vendor adds the detection strings for new, just discovered viruses. Updating is a 24 x 7 service which requires no intervention by our staff.

Reminder

Remember, only the email you receive in your central email account's inbox is scanned for viruses. Viruses can find their way to your computer in many other ways, such as:

- Files you download via your Web browser or FTP.
- Some inboxes are maintained on departmental mail servers. (If you use a departmental email server for receiving your mail, check with your email administrator to learn about options the server supports.)
- USENET NEWS (news.umn.edu)
- Infected disks you insert into your computer.

If you turn on the "forward" option for your centrally assigned TC email, you no longer receive mail at that internetid.email.umn.edu address. So, unless you forward the mail to another centrally assigned TC account, the email doesn't get scanned by OIT's software. (You can turn the forward option on and off via this Website: <http://www.umn.edu/validate>)

We strongly recommend that you install and maintain up-to-date virus detection software on your own workstation. A multi-layered approach to this threat is the most effective way to avoid infection.

■ Frank Grewe, Office of Information Technology

Is Big Brother Watching You in the Library?

Nancy K. Herther, University Libraries, <http://www.lib.umn.edu>

Newspapers carry stories daily about incidents, technologies or possible privacy issues related to computer technology and the Internet. Below are a few recent examples.

★ **TiVO** is a company that sells computer-based video tape systems that are capable of recording all of your usage; and since it plugs into your phone system in addition to downloading TV schedules to the box, it can upload information back to TiVO on every keystroke you use. The company now admits to gathering consumer information this way in violation of its own online privacy policy.

★ **Full-page ads** ran in the May issues of *New Yorker* and the *New York Times Magazine* in which the ACLU warns that government e-surveillance programs like “Carnivore” and “Echelon” are encroaching on Fourth Amendment protections against “unwarranted government surveillance.”

★ **“Location-based commerce”** is a new concept based on the ability of technology to pinpoint the exact location of wireless users. Using this information, some companies propose to automatically send cell phones or computer/palm devices advertisements as people come into a specified physical range close to some business. Another concern here, of course, is who’s keeping track of the data on the physical movements of people with wireless equipment as they move about each day.

★ **“Web bugs,” invisible images** on a Web page, are being used by marketers to signal to sites other than the ones you’re visiting to put a “cookie” on your computer. To gauge the prevalence of Web bugs, Intelytics recently scanned 51 million Web pages and found tracking devices on

nearly one third. It found that 74% of the top 100 e-commerce sites had bugs that tracked visitors from third-party Web sites.

★ **A Georgia company admits** to having electronically recorded everyone entering Raymond James Stadium to watch this year’s Super Bowl — now being called “Snooper Bowl” in the press — and then matched these pictures, using face-recognition software to faces of known criminals and suspected terrorists in a law-enforcement database. The Rand Institute recently reported: “Sensors will be everywhere, including tiny wireless video cameras and microphones.”

Incidents such as these make us all wary of the power of technology to invade the privacy of us all. Every day the media is filled with articles and news bites related to privacy.

During the week I wrote this article there were over 125 articles on “Internet” and “privacy” in a single week in the US NEWS newspaper section of Lexis-Nexis. A variety of organizations and research centers have arisen to study and track these issues as well.

See Figure A at the end of this article for some Web-sites worth checking out.

Big Brother



“The head of state in George Orwell’s novel 1984; hence, an apparently benevolent, but ruthlessly omnipotent, state authority.

Also attrib. Hence Big Brotherdom, the rule or position of Big Brother; Big Brotherism, behaviour characteristic of Big Brother; Big Brotherly a., of or pertaining to Big Brother.” — Source: OED Online

U Libraries policy

The University Libraries has a firm, unwavering commitment to academic and intellectual freedom. Sometimes this requires a great deal of thought and work on our part to guarantee your right to access information as well as keep the necessary “business” of libraries free of any record keeping or processes which might compromise your rights.

Questions

Recently I’ve received a number of questions from users that may involve issues that you might have as we continue to automate many of our services. I’ve gone to the experts here in the Libraries to get the answers. Here they are:

Q1: How private are my circulation records? Do you keep track of all of the books I’ve checked out?

A1: The privacy of circulation records is protected by Minnesota statute. When an item is returned, the online system no longer displays the item charged out on the patron’s “has” list and there is no longer an online link between the item record and the patron record. During the period when the item is charged to a user, authorized Library staff do have access to the record. Each year these staff sign confidentiality agreements to assure user privacy.

★ “The freedom to read is about choice and respecting the right of others to choose for themselves and their families what they wish to read. It is one of the most precious freedoms we have in a democratic society. Book banning and challenging has a domino effect. If we stand quietly by and let the first book come off the shelf, we run the risk they all will come tumbling down.” ★ From a statement of the American Library Association (ALA)

Q2: Why do the databases time out?

A2: Many of our databases and e-journals are purchased via a site license that allows the University of Minnesota-Twin Cities a specific number of simultaneous users. Only a certain number of students and staff are allowed in at any one time. This is often the only way the Library can afford to provide electronic access to some resources (unlimited access being prohibitively expensive).

★ “I believe in censorship. I made a fortune out of it.” ★ Mae West (1892 - 1980)

Q3: How do the databases decide when to “dump” me?

A3: When you’re “dumped” you get a message like this: “Your session has timed out. Please try again later.”

In order to allow others access to the system the computers are programmed to log you off whenever there is, usually, about fifteen minutes of inactivity. This is necessary because so many of our contracts only allow “x” number of users to use a particular database at the same time. If we didn’t do this, a person could log on and stay on some database indefinitely, preventing others from having fair use of these resources.

★ “Censorship, like charity, should begin at home; but, unlike charity, it should end there.” ★ Clare Booth Luce

Q4: Do the Libraries use cookies to track how people use the Libraries’ Web resources? If so, do you keep information on individuals or do you delete this?

A4: The Libraries make limited use of cookies but not to track how people use the Libraries. We use cookies to “maintain state” — or remember key settings that you choose — to make your Web session run more effectively so you don’t have to retype information, as

we do in the “Contact Info” part of our interlibrary loan forms, etc. This information is not kept or shared with anyone.

✳️ **“Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightenment.”** ✳️ **American Library Association Library Bill of Rights**

Q5: Do the commercial databases that you use keep track of my searching? Do they keep track of which databases I’m using?

A5: Database vendors do have software that tracks users in order to determine if there are any obvious copyright infringements taking place.

A few years ago a student tried to download all of the articles from a particular issue of some journal. The vendor’s software programming picked this up immediately and cut off the student’s access to the database. This was a clear copyright infringement.

Vendors do collect baseline statistics on things like the numbers of searches and numbers of articles displayed and probably the search terms entered. These sorts of impersonal data help the vendor improve the product by seeing how and what is being used, etc. Each vendor would have their own procedures and software. However, in our contractual negotiations, the Libraries – and any library – would require language guaranteeing the privacy of our users.

✳️ **“Intellectual Freedom is the right of every individual to both seek and receive information from all points of view without restriction. It provides for free access to all expressions of ideas through which any and all sides of a question, cause or movement may be explored. Intellectual freedom encompasses the freedom to hold, receive and disseminate ideas.”**

✳️ **American Library Association, Intellectual Freedom and Censorship Q & A**

Q6: If I use the computers in the Libraries to do my research, are there ways vendors can tell who I am? Or am I anonymous?

A6: When you log in with your InternetID and password, these pieces of information are not passed to the database/e-journal vendor. They are merely checked against the publicly available University of Minnesota Student-Staff Directory to ensure that you are a current U of M affiliate.

From this transaction all the vendor knows is whether or not your computer’s IP number belongs to the U of M-TC campus. (You can access the directory at this Website: <http://www.umn.edu/lookup>.)

✳️ **“Restriction of free thought and free speech is the most dangerous of all subversions. It is the one un-American act that most easily defeats us.”** ✳️ **Supreme Court Justice William O. Douglas**

Q7: I was timed out in a database. Does the vendor have a record of all the subjects I was searching?

A7: The policy of the University of Minnesota Libraries is to respect and protect the privacy of the students, staff, faculty and other users. To ensure network security and consistent service for all users, software programs may be used to monitor network traffic, identify unauthorized access or access to non-public or restricted information and detect viruses and other software that might cause damage to the network. In addition, the Libraries may periodically collect and store information to help manage our Websites and to improve service.

Personally identifiable information from these activities is not released to external parties unless required by legal proceedings or law enforcement. Vendors, publishers and other external suppliers of digital information resources with whom the Libraries have contracts for access may collect information for the same purposes. Our contracts with the external vendors prohibit them from distributing or selling this information.

All data collection is governed by the Federal Privacy Act and Minnesota State Statute.

✦ **“We uphold the principles of intellectual freedom and resist all efforts to censor library resources.”** ✦
American Library Association Code of Ethics

Q8: I wanted to use the new Web-based Interlibrary Loan (ILL) form, but I don't want people to track the materials I'm requesting. Does anyone get to see what materials I have ordered through ILL?

A8: Information submitted on the ILL Web form is secured from hackers while the request is in-transit.

Requestors of interlibrary loan and document delivery services receive the same protection in terms of the confidentiality of their requests as they do with their circulation transactions.

In some cases, information about requests is shared with other Library staff for collection development purposes; this information remains confidential within the Library. Documentation of requests may be retained as necessary for the Library to comply with auditing, copyright or other regulations.

✦ **“Congress Shall Make No Law Respecting an Establishment of Religion, or Prohibiting the Free Exercise Thereof; or Abridging the Freedom of Speech, or of the Press; or the Right of the People Peaceably to Assemble, and To Petition the Government for a Redress of Grievances.”** ✦ **First Amendment to the United States Constitution**

Q9: When I connect through MNCAT to an outside database, are they keeping track of who I am and what I'm doing? What about links to outside Websites?

A9: Web MNCAT is the University Libraries catalog of holdings.

The Web MNCAT software, which includes standard Web server software and library interface software, includes the ability to maintain numerous log files. Many of the log files are only enabled to troubleshoot system problems. Other log files are continually maintained as part of best practices for server administration.

If our servers became a victim of hacker or denial of service (DoS) attacks, this information would assist campus networking security and law enforcement to potentially identify the source of the attack. Any tracking by the Library of which links were followed in Web MNCAT would be in the form of generalized information, for example, to identify which resources were more frequently accessed from within Web MNCAT.

URLs within MNCAT refer to two primary types of resources. One type is those explicitly purchased and licensed by the University for current University students, faculty and employees. Examples include:

- full-text journals (for example Academic Press: <http://www.idealibrary.com>)
- indexing and abstracting services (for example Digital Dissertations: <http://www.lib.umi.com/dissertations/>)
- full-text reference sources (for example Oxford English Dictionary: <http://dictionary.oed.com/entrance.dtl>)

As noted in the response to Question 4, the privacy of our users is a component of these licensing agreements.

Another type of resource is those freely available resources that have been included in MNCAT. Since there is no explicit agreement regarding access to these resources, using them would be no more or no less secure than general Web browsing. Government publications and databases make up a large share of the freely available resources.

✦ “The right to be let alone is indeed the beginning of all freedom. ✦
Justice William O. Douglas

Q10: Do the Libraries have policies that outline my rights in using computer resources?

A10: University Libraries’ Appropriate Use of Computer Workstations and Electronic Resources policy is our statement of support for the free flow of ideas and the serendipity of thought in our networked environment. The policy can be found at:
<http://www.lib.umn.edu/appuse.phtml>

Our Library is a proud member of the American Library Association and its policies and principles on intellectual freedom can be found at:
<http://www.ala.org/work/freedom/lbr.html>

✦ “Morals are private. Decency is public.” ✦ Rita Mae Brown, “Starting from Scratch: A Different Kind of Writer’s Manual”

Q11: When I log into the databases I enter my userid and password. Is that information being kept someplace?

A11: Your University of Minnesota InternetID (sometimes called userid) and password are only used to query the campus x.500 directory service so that the Library can identify whether you are a current University student or employee for purposes of inclusion under our license agreements with the resource providers (that is, the electronic book and journal publishers).

The Library does not retain this password information beyond the point of validating your access rights.

✦ “Everything that is really great and inspiring is created by the individual who can labor in freedom. ✦
✦ Albert Einstein (1879–1955), ‘Out of My Later Years,’ 1950

Essays on intellectual freedom

One of the library profession’s greatest defenders of the first amendment was a former professor and department chair of the University’s one-time Library School.

David Berninghausen, who passed away on April 4, 2001, was an unwavering First Amendment supporter and one of the reasons that I, personally, decided on this field.

Check out his thoughts in this classic book (available in Wilson Library): *The flight from reason: Essays on intellectual freedom in the academy, the press, and the library* by David K. Berninghausen. Chicago: American Library Association, 1975.

Q12: I use Current Contents and have set up a profile so I can have the searches automatically run and sent to me. Who keeps my profile? Who is able to see this information?

A12: The Current Contents database is hosted by the Bio-Medical Library as part of its BiomedSearch Ovid service. Other databases are also available, such as Medline and CancerLit.

The very first time a user logs on to the Bio-Med Ovid server using their campus InternetID, a home directory is created, behind the scenes, for that user. If a user creates any profile information or stores search strategies while using the databases on the Bio-Med Ovid server, that information is stored in the user's home directory.

A search strategy is simply a series of search commands that produces a search result that is pertinent to the user's information needs.

By storing a search strategy as a file on the Ovid server, the user can re-use the strategy later on. This can be a real timesaver, and many Ovid users save dozens of search strategies. When saving a search strategy, a user can select the AutoAlert (SDI) function whereby the search strategy is re-run automatically against new database updates. In the case of Current Contents, users who have selected this service receive weekly email messages from the Ovid server supplying new hits for the previously stored search strategies.

Information stored in a user's home directory is considered confidential and private. This includes all search strategies, whether SDI or not. No one has access to this information other than the systems administrator.

In rare situations only, and in response to changes in the Ovid system, the systems administrator might view and edit a search strategy or change a profile. In this way, the system administrator is making sure that user profiles continue to work in a system that is growing and changing every week.

User confidentiality is a basic operating principle behind the BiomedSearch service provided to the University community.

✳️ “Freedom is not worth having if it does not connote freedom to err. It passes my comprehension how human beings, be they ever so experienced and able, can delight in depriving other human beings of that precious right.” ✳️ Gandhi, 1931

Q13: My professor told me to talk with the bibliographer for my subject. Will s/he report this back to my instructor?

Are instructors told who attends Library workshops or classes?

A13: Occasionally students may feel awkward about talking to librarians about their research questions – whether the research is for personal, professional or school use. All librarians hold tightly to the first amendment principles of free expression and academic/intellectual freedom. We also believe firmly in our fiduciary responsibilities to maintain the best interests of our clients and to protect their interests.

If you meet with staff or ask questions (any questions – believe me there are **no** “dumb” questions), this information is treated with the same type of respect that any professional would expect.

We do not maintain records of our reference/research work beyond, generally, keeping “hash” mark statistics on the numbers of questions we answer each hour or day.

We do not report to faculty on student attendance at instructional sessions or workshops or on students contacting us for assistance in doing their secondary research work. Certainly there are cases in which faculty attend the sessions and, then, they may take attendance.

Many librarians do, however, establish long-term relationships with faculty and (generally graduate) students involved in complex research projects. Certainly, in this case, some records and information may be kept in order to help with ordering materials or checking facts/information. However, this information is also kept confidential.

✦ “Follow the path of the unsafe, independent thinker. Expose your ideas to the dangers of controversy. Speak your mind and fear less the label of ‘crackpot’ than the stigma of conformity. And on issues that seem important to you, stand up and be counted at any cost.” ✦ Thomas J. Watson



Silent partners

The Libraries are a vital partner in the instructional and research programs here on campus. However, in most cases we tend to be “silent” partners, facilitating the process of secondary research and, hopefully, helping to further scholarly research in general.

If you have any questions or concerns about some research you need to do, talk to us. We are available 24x7 via email, voice mail or the Web. In addition the Libraries have a full-set of reference service hours throughout the calendar year. We have specialists in every library who would be happy to meet with you in one-on-one consultation sessions if that would be a more comfortable way to approach your research.

Have a question? Just ask us!

Go to the *AskUs/InfoPoint* section of our Web page to fill out an electronic message (and remain anonymous if you wish) at: <http://infopoint.lib.umn.edu/>

Or feel free to stop in at any reference desk or call. Information is power, and we’re here to help you in any way that we can!

■ Communications about this column should be addressed to: Nancy K. Herther, Social Sciences Bibliographer, 170b Wilson Library, West Bank; 612-624-2020; n-hert@umn.edu

Figure A: Want to learn more about privacy issues?

For more information on digital technology, privacy and other key issues, check out these Web sites:

- Digital Futures Coalition:
<http://www.dfc.org/>
- Electronic Frontier Foundation (subtitled “Protecting rights and promoting freedom in the electronic frontier”):
<http://www.eff.org/>
- Georgetown Internet Privacy Policy Study:
<http://www.msb.edu/faculty/culnanm/gippshome.html>
- Yale Law and Technology Society:
<http://lawtech.law.yale.edu/>
- The Privacy Foundation:
<http://www.Privacyfoundation.org/>
- Electronic Privacy Information Center:
<http://www.epic.org/>

The policy of the
University of
Minnesota Libraries
is to respect and
protect the privacy of
the students, staff,
faculty and other users.

Summer Savings from TechMart

On April 20, 2000 the University introduced TechMart, a new service that lets students, staff, faculty and departments purchase computer equipment online via the Web. Since then we've added more services and bargains to TechMart. And we're negotiating with more vendors to add more services.

This summer look for coupons and other specials in the TechMart Quarterly, a newspaper-style publication available in special news racks in over 100 campus locations.

TechMart basics

Q: What is TechMart?

An online store that offers educational discounts for computer and information technology products and services.

Q: Who can purchase through TechMart?

Current students, staff, faculty and departments of the University of Minnesota. Alumni are not eligible to purchase through TechMart.

Q: What is the difference between department and individual purchases?

Department purchases are those made with a purchase order using University funds. Individual purchases are those made with personal funds.

Q: Where can I get more information about TechMart?

TechMart website: <http://www.techmart.umn.edu>

Frequently asked questions

Q: Is shipping free?

Sometimes it's free.

- Apple: standard ground shipping is free for both department and individual (student, staff and faculty) purchases. However, if express shipping is chosen, there is a charge.

- Dell: standard ground shipping is free for department purchases only. Those making individual purchases must pay ground shipping charge of \$45 on Desktop systems and \$30 on Notebook systems. Express shipping is more expensive.
- Unique Software: shipping charges apply for both department and individual sales and the charges depend on the items ordered.
- Gateway: shipping charges apply. For Desktop systems the charge is \$80 and for Notebooks it is \$35. Express shipping is more expensive.

Q: Can I get the UM discount for DSL and/or cable modem access even if I am already signed up for it?

Yes, provided you are a current student, staff or faculty member at the University of Minnesota.

- To get the University DSL discount, send e-mail to <TechMart@umn.edu> that includes this information: your name; the name of the Qwest account holder; and complete phone number. In the e-mail explain that you have DSL service through Qwest, and you would like to get the University of Minnesota discount. The rate change will be effective immediately, and in approximately six weeks the credit will appear on your bill.
- To get the University cable modem discount, go to TechMart's cable modem link: www.techmart.umn.edu

Then from this link sign up as if you were ordering High Speed Access for the first time. After you click on the "Send it in" button, you will be asked to put in your University of Minnesota InternetID and password. AT&T RoadRunner will receive your request and change the billing on your cable service bill. The rate change will be effective immediately. In approximately six weeks the credit will appear on your bill.

Q: How does B2B and Financial FormsNirvana work?

To use the department sites for Apple and Dell (and in the future all vendors), you must be set up to create purchase orders using Financial FormsNirvana (FFN). If you are not set up to use FFN, talk to your Resource Responsibility Center (RRC) manager about getting set up to use FFN.

When you place an order on one of the Business to Business (B2B) vendor sites, you must use your Enterprise Systems password to log in. This will allow you to start FFN at the end of the order process. When you shop at a B2B enabled site, your shopping basket will be transferred to an FFN purchase order with the Vendor Code, Contract number, line total and unit price fields already completed! Simply complete the rest of fields, such as ILOC code, CUFS numbers, approver and submitting division. Click on "Submit request," and you are done placing the order.

Once approved, the purchase order will be sent to the vendor electronically. This does not mean payment will be sent electronically. When you receive an invoice, you must attach a payment voucher to the invoice and send it to disbursements.

Q: What laptop/monitor/scanner should I buy?

You can contact the Technology Helpline at 612-626-4276 if you need advice on what to look for when you make your purchases. For reviews and recommendations about personal computers and peripherals, such as scanners, a good Website to go to is: <http://www.zdnet.com>

Q: How do I purchase software?

Currently you can select Unique Software Corporation to buy software at academic pricing. And Apple software, along with other selected software, is available through Apple.

Q: What vendor sells scanners? printers?

Unique Software Corporation, Apple Computer and Dell Computer Corporation all sell selected hardware peripherals.

Q: How long will it take to get my order?

It can take as little as one to three days or as long as three to four weeks. The length of time before you actually receive your order depends on the items you ordered. Most computer systems are built to order and can take one or two weeks to ship. Software and peripherals typically ship more quickly. Other factors that affect delivery time are availability, shipping method and the location the item is shipped from.

For department purchases, the time it takes for the purchase order to be approved is also a factor.

■ Tips from the Technology Helpline

Information Technology Newsletter Subscription Request

Add to paper copy mailing list.

(You can also email this information to: oitnsltr@tc.umn.edu)

Name _____.

If University of Minnesota Twin Cities Campus Mail:

■ Use your departmental mailing address. Do not use your personal office address.

■ *Optional:* Include Campus Mail Code: <http://umn.edu/lookup>

Department _____.

Department Mailing Address _____

If U. S. Postal Service:

Address _____.

_____.

City _____ State _____ Zip _____

You can **FAX** the coupon to 612-625-6817.

Published monthly by the Office of Information Technology, editor, Mary Kelleher, <oitnsltr@tc.umn.edu>.

Paper subscriptions are free but are mailed only within the USA. Electronic versions are available on OIT's website as HTML (web) and PDF (Acrobat) documents: <http://www.umn.edu/oit/newsletter>

For alternate subscription information, see: <http://www.umn.edu/oit/newsletter/subscription.html>

▼ Help

Phone: Area Code = 612

Computer Misuse or Abuse (also see Procedure 2.8.1.1)

- Emergency Network Help Line 625-0006
- Non-emergency, e.g., spamming: abuse@tc.umn.edu

1 Help • 7/24/365, unless otherwise noted 301-4357

■ CCO: central systems, PeopleSoft

- Web: <http://www.umn.edu/cco>
- by email: x-help@cafe.tc.umn.edu

■ Internet, Email, Microcomputers, Distributed Systems

- call-in Monday–Thursday • 8 am–11 pm
- call-in Friday • 8 am–5 pm
- call-in Saturday • noon–5 pm
- call-in Sunday • 5 pm–11 pm
- walk-in 8 am–5 pm, M–F:
152 Shepherd Labs; 93 Blegen Hall; 50 Coffey Hall
- Web: <http://www.umn.edu/adcs>
- by email for U of M: help@tc.umn.edu

■ Passwords: new and forgotten ones

■ NTS-TAC: Technical Assistance Center

- Web: <http://www.umn.edu/nts>

▼ Dial-in Computer Access

Internet/PPP/SLIP: up to 53kps if v.90 612-627-4250

(56k K-flex, Flex56, X.2 protocols are unsupported)

Modem Usage (current activity on your account)

www.nts.umn.edu/services/modemusage.html

▼ Web and Internet Addresses

Quick Guide

Information Technology Newsletter

<http://www.umn.edu/oit/newsletter>

Internet/Email account management/validation

<http://www.umn.edu/validate>

MNCAT/LUMINA (Library) – <http://www.lib.umn.edu>

Office of Information Technology

<http://www.umn.edu/oit>

Onestop Services – <http://onestop.umn.edu>

TechMart – <http://www.techmart.umn.edu>

UM News Server – news.tc.umn.edu

▼ General

Phone: Area Code = 612

Threats, UM Police Department 911 on campus

- off campus 624-3550

Technology Training Center 625-1300

- web: <http://www.umn.edu/adcs/info/training.html>

Computer Accommodation Program – voice/tty... 626-0365

U Computer Services/Computer Repair Serv 624-4800

Digital Media Center 625-5055

Statistical Software Support:

- including SAS and SPSS 624-3330

Associate Vice President and

Chief Information Officer, Steve Cawley 612-625-8855

Newsletter subscription information and archives at <http://www.umn.edu/oit/newsletter>

©2001 by the Regents of the University of Minnesota. All rights reserved. The University of Minnesota is committed to the policy that all persons should have equal access to its programs, facilities and employment without regard to race, color, creed, religion, national origin, sex, age, marital status, disability, public assistance status, veteran status or sexual orientation. This publication is available in alternative formats upon request.

Twin Cities campus address label trivia: the 2nd number after the Rec# is the Campus Mail delivery code, <http://umn.edu/lookup>

Jun.2001 [pantone295,1205]

Delete/Cancel

Change Name

Change Address

Change Other

Add

If you cancel or change, please tell us the Rec#.

Just tear off the end page and send the entire mailing label to us. Or send email to: oitnsltr@tc.umn.edu

Nonprofit Organization
U. S. Postage
PAID
Minneapolis, MN
Permit No. 155

Information Technology Newsletter
University of Minnesota
Office of Information Technology
190 Shepherd Labs
100 Union Street SE
Minneapolis, MN 55455-0421

