

## News from IT – 01/30/04



### New Virus Pounding the Internet-

A fast-spreading virus, "myDoom", has been making its way through the cyber world at an accelerated rate over the past several days. A variant, "myDoom.B" with even greater potential to do harm, has also been observed.

Fortunately, virus defenses on the campus mail server and desktops have thus far stopped "myDoom" from compromising University systems. The side effects of myDoom have and will continue to cause email related issues, as well as significant slowdowns in various portions of the Internet. Since this virus is fast moving and quickly multiplying, it has more than tripled the amount of mail traffic to campus. In addition, the virus "spoofs" sender addresses, causing users to receive "Undeliverable" warnings from servers, reporting that you sent out an infected message, when, in fact, you have not.

IT is attempting to temporarily hold all "Undeliverable" returns until the brunt of this virus attack is over. You may experience slow Email retrieval and delays in accessing Internet sites.

For more information:

<http://www.cnn.com/2004/TECH/internet/01/27/mydoom.spread/index.html>

The presence of "myDoom" and other viruses further underscores the importance of keeping virus protection current in academic, residence hall and home computers. Hackers, always alert for new opportunities, have used security holes opened by this virus to install such software as key loggers and spam relays on infected machines. If you carry a laptop between home and campus, please insure your virus protection is up-to-date and used regularly to scan the entire hard drive for viruses. Enable "mail scan" if your virus protection product suite is so equipped. For more information on protecting your home computer, refer to the article on this subject archived from the September, 2003 issue of *the News*:

[http://it.mnsfld.edu/policies/itnews\\_archive/NewsSept03.pdf](http://it.mnsfld.edu/policies/itnews_archive/NewsSept03.pdf)

### IT Quarantines Attachments To Stem Viral Tide –

With the recent spread of the Bagel and my.Doom viruses, as well as the "FDIC" and "PayPal" Scams, IT has implemented a new system to quarantine potentially harmful and nuisance emails that may spread

rapidly before virus and spam defenses are able intercept the threat. Effective immediately, emails containing potentially harmful attachments will be sent directly to a “\_Quarantine\_” folder of your account. The “\_Quarantine\_” folder is only accessible from the web interface, and as a result, potentially harmful messages and attachments will not be retrieved automatically by your Eudora or other desktop mail client.

If you are expecting an email from a known source with attachment type in the quarantined group (for example, a .zip file), you may access your account via web access and retrieve the document. Documents in the “\_Quarantine\_” folder will remain there for 30 days. In addition to attachments, messages originating for “Postmaster” or “mailer-daemon” accounts will also be sent to the “\_Quarantine\_” folder. This has been done because a majority of returned mail is generated by viruses such as my.Doom, so.Big, and others which “spooF” Email addresses.

PLEASE NOTE THAT NORMAL ATTACHMENTS AND DOCUMENTS FROM WORD, EXCEL, POWERPOINT, PDF FILES, TEXT FILES, AND IMAGES (JPEGS, GIFS, TIFFS, ETC.) **ARE NOT AFFECTED**, AND WILL BE RECEIVED NORMALLY!

If you have any questions, please contact the Helpline at 4357. The lists of quarantined extensions are listed below:

- \*.zip
- \*.exe
- \*.bat
- \*.cmd
- \*.reg
- \*.vbs

(\* .scr, \*.pif, \*.lnk files are banned. Attachments with these extensions are immediately deleted, as they are only used to deliver viral payloads.)

## Net Registration Implemented for Residents –

By now, most of you have heard about the battle between the RIAA, the Recording Industry Association of America, and users of file sharing services like Kazaa. IT has expended significant time and resources over the past few years complying with our legal requirement to identify users of our network sharing copyrighted materials. As other people, such as the movie industry and other copyright holders get into the act of leveraging Federal Law to force service providers to supply investigative resources, honoring these requests in a timely manner has become a significant burden to our networking group, with no real benefit to us or

our users. In an effort to ease this burden as well as to better manage our network resources, network registration became a prerequisite to obtaining Internet access in the Residence Halls beginning with their opening this semester. Every network interface card carries a unique identification number associated with all data traffic sent from that station. Student users of our network, upon initial connection, receive a screen from the NetReg system which they must fill out, identifying them as the owner of that particular computer. Subsequent connections are compared against known users, and if the user has already been identified to our network, they are automatically allowed access to the Internet. IT wishes to recognize our newest team member, Calissa Lazowicki, both for her recent certification in Linux systems, and significant contribution to the successful implementation of this tool. Calissa and others on the network team will continue to add services to NetReg over the coming weeks.

## SAP Implementation Reaches Mansfield –

The Shared Resource Enterprise Administrative System, powered by SAP, has arrived. This project, intended to provide a common resource for the State System Universities, is now powering the University's Financial, Purchasing, Human Resources and Payroll systems, replacing Datatel in those specific areas. Implementation was primarily handled by the user areas involved in specific applications, and has gone well.

## Phase I of Campus Security Updates Frozen in a Nearly-Completed State-

Through the combined efforts of Buildings and Grounds and Information Technology, significant updates to campus security were implemented during November and December. Phase I plans called for the installation of 15 security "Blue Light" phones around the campus. Pressing the HELP button on any of these instruments results in the activation of a 2-million candlepower strobe light and immediate connection to 911 Emergency Services. All security phone locations have been mapped into Tioga County's emergency database, so the exact location is available to be relayed to the nearest available emergency responder when a call is received. Thirteen of the 15 phones planned for Phase I were successfully installed prior to cold weather. An additional phone, planned for Phase II, has also been installed and is awaiting final connection, also delayed by severe weather. Additionally, the Turkey Path has been equipped with security cameras, with monitoring of the South Hall Mall area planned in parallel to emergency phone installation there, now scheduled for spring.

A further planned enhancement is direct attachment of the University's internal telephone network to 911. A request-for-proposal is now on the

street, with bid award anticipated around the end of February. This enhancement will provide exact location information for every telephone on campus, with simultaneous 911 alerts occurring at County Communications and the office of Campus Police.

## IT Shifts Resources –

As a result of the University's Budget Reduction Plan, IT has reassigned staff to better serve our overall campus mission. This may have resulted in your building technician being reassigned to another area. You can find out who your tech is by consulting the IT web pages:

<http://it.mnsfld.edu/client/> or by calling the HELP desk.

## A Call for New Products –

Let this be your first notification! Friday, March 12 is the *last* day to request consideration of new products to be included in the university's suite of supported software for summer and fall 2004. While IT does not FUND new software requests, we must know about them in order to verify functionality alongside all the other products we must support, as well as to schedule implementation time. Your requests should include CD-ROM titles included with textbooks. Questions and your requests should be directed to Alex Miller: [amiller@wheat.mnsfld.edu](mailto:amiller@wheat.mnsfld.edu).

## In Other News... -

IT has been very busy with other projects around campus. Unless otherwise noted, all projects are, in whole or in part, funded through Student Technology Fees. Here are the highlights:

\* \* \* \* \*

State Farm Insurance has granted funding for an exciting new high-tech lab for the Department of Mathematics and Computer Science. Paired with funding obtained from Student Technology Fees, the new lab will be a hands-on resource for teaching networking fundamentals and demonstrating network security concepts.

\* \* \* \* \*

A new graphics facility will be available in the North Hall Library after spring break. The new graphics work stations will replace student access previously supported by Media Services in Allen Hall. The new facility extends the hours in which services are available for students doing posters, scanning, and other class assignments requiring imaging services.

\* \* \* \* \*

Plans have been finalized for a digital music lab, to be constructed in Butler Center during the spring and summer, with availability in time for fall '04 classes. Equipment and furniture are on-order, with delivery anticipated sometime in March.

\* \* \* \* \*

Another small lab, this one for the use of commuter students, will be built this semester in the Alumni Hall Student Union. The lab will also double as a space to be used for pre-registration in the spring, and during Orientation sessions over the summer. Connectivity in AHUB will be further enhanced by the inclusion of wireless networking connectivity in the area of the lab.

\* \* \* \* \*

IT is working with the Library on an exciting new service. An electronic music reserves system is being developed which, it is hoped, will be available by fall '04. An in-house server and software will be used to categorize and digitize musical selections, which will then be made available as part of a searchable data base on the campus Intranet.

\* \* \* \* \*

IT continues to enhance and integrate technology carts in all classrooms seating more than 25. Four new cart systems were added to Grant over Christmas break. Upgrades to specific rooms for faculty who have expressed an interest in Mimio technology – a scanning technology allowing white board images to be digitally recorded on the cart's PC and stored for future retrieval – are currently under way. Another round of new cart systems is being constructed now. These systems are a special emphasis project supported by Provost Lane.

\* \* \* \* \*

Finishing touches to hardware upgrades are being completed by Dr Thorne to the Geology and Geography Lab, located in Belknap Hall.

\* \* \* \* \*

## Spyware Remains a Significant Problem on Campus Computers-

We talked about this in the September issue of *the News*, but from what we're seeing, our advice has largely gone unheeded, and bears repeating:

Many on campus, and certainly some at home are plagued by personal computers that stall, crash, and perform poorly. What IT continues to see is the presence of "tools" purported to help you maintain your PC or move around the Internet faster and safer. These tools, with names like Hotbar, Xuiper, Gator, Date Manager, Time Manager and Weather Bug, once installed on your machine, dramatically affect its performance and reliability. A typical Help desk call reports that an affected machine has become so slow and unstable that you demand that we *DO* something, *anything*, to fix it. IT visits your office and works our magic - things are better, you are happy and off surfing again - probably again doing all the stuff that got you in trouble in the first place.

This morning, one of our techs took a call on a machine that was giving Fatal Exceptions, was very slow and having a hard time opening common tasks, reporting "out of space to perform (this) operation." Why? This particular machine had Hotbar, Xuiper, LOP Search, Win Search Tool, and Win Enhancer Tool loaded on it. These five "tools" had been voluntarily loaded with the intent of enhancing the user's Internet experience. But the sad fact is, none of these tools performed as-promised, and the loss of system resources by their very presence made this person's personal computing environment far more prone to crashes and stalls, as well as preventing our virus scanners and other automated cleanup tools from running.

What is actually happening here? Products such as Gator, Date Manager, Time Manager, and Weather Bug are, in fact, Trojan Horses, offering up some purportedly desirable service, when in actuality their purpose is to follow your every move on the Internet and report your surfing habits to 3<sup>rd</sup> parties, whose intent is to sell personal information to advertisers.

Some of these products sneak in through a "back door" simply by surfing to a less-than-scrupulous web site. *Most are installed by you, the user, because you clicked on a pop-up that promised something for nothing.*

What is IT doing about this? Taking our users, particularly repeat offenders, out and shooting them has previously been vetoed by senior IT

staffers. With the most obvious solution unavailable, we've had to rely on software, and have provided SpyBot to each and every desktop on campus. SpyBot will run automatically when you log-in Monday mornings. This program will remove most known spyware, and prevent most new infections from getting to you, *but the product must run to completion in order for it to clean your machine, and repair the damage*. If your machine was compromised prior to our delivery of SpyBot, it's possible that multiple versions of installed spyware may actually prevent it, and our virus scanners, from doing their job.

Remember: These rogue programs are much like the viruses we encounter, once someone figures out how to stop one, the bad guys develop new, more sophisticated ways to get to you. The open structure of the Internet and quality of PC software insures there will always be "windows of opportunity" (no pun intended) for hijackers and viruses. IT places a high priority on preventing these problems from occurring on your machine, but the bad guys are doing their best to compromise *you*. You must practice vigilance and use common sense to insure a secure and safe computing experience. Refer to the September '03 issue of the *News* for more information on products you can use to secure your home computer.