ITS Information & Technology Services news

The official source of news from ITS Information & Technology Services

December 2002

Computer Network Security Awareness: A Global Issue that Touches RIT

By Diane Barbour, Chief Information Officer, dhbcio@rit.edu

Information Security is a high priority for RIT and Information and Technology Services (ITS). As a result, we have devoted this issue of ITS News to Information Security – practices and safeguards.

With the events of 9/11/01 and the rise in cybercrime, security has become a national issue. President Bush's Critical Infrastructure Protection Board is creating a national strategy to secure cyberspace. The strategy includes a special section for Higher Education.

The Plan calls on colleges and universities to aid in securing networks by developing network safeguards to protect computers from online attacks. The report states that "colleges and universities have large computer labs, high –speed Internet lines, and state-of-the-art computer equipment – all of which are open to many users".

In this issue of ITS News you will read about the steps that ITS has taken to ensure security on the RIT network. You will also read about what steps you can take to improve the security of your own computer as well as how to report incidents of computer and network abuse.

I urge you to read this issue carefully and take whatever action is necessary to secure your personal computing environment.

"Each time you or I use the RIT network, we are 'In an inescapable network of mutuality…whatever affects one directly, affects us all indirectly.' Not only do our actions on a connected computer impact people connected to the RIT Network, but there is the potential for our actions to impact anyone connected to the Internet. We become part of the global community." (D. Cullen,* Privileges and Responsibilities Defined in the Computer Code of Conduct*, pg. 8)

R·I·T

ITS News

Balancing Intellectual Freedom, Privacy and Security

By Dan Tobin, Associate Director, Enterprise Technologies and Architecture, Technical Support Systems, dbtits@rit.edu

RIT has a long history of implementing technologies to provide a rich learning environment for both students and faculty. Liberal access policies provide connectivity to institute resources both on and off campus. As a result, many institutions of higher education, incluidng RIT, are *on the Internet*, without the blanket of protection provided by firewalls at our Internet borders. Ease of access to campus systems, combined with high speed internet connections, make RIT a prime target for hackers looking to compromise, control and then use computing resources.

The events of 9/11 have put into motion a new awareness and sense of urgency around securing the United States' technical infrastructure. This includes the Internet and Internet accessible devices. In support of the *National Strategy for Homeland Security*, the *President's Critical Infrastructure Protection Board* has drafted "The National Strategy to Secure Cyberspace." Although this strategy is still a draft document being circulated for comment, it already identifies Institutions of Higher Education (IHE) as an area of focus.

What does this mean to ITS and RIT?

Although IHEs are identified specifically because of their computing power, ease of access and high speed internet connections, the strategy generally falls short of spelling out specific steps to be taken by institutions. It also does not attempt to set a baseline or detail any cybersecurity benchmarks by which IHEs will be measured.

> *"The events of 9/11 have put into motion a new awareness and sense of urgency around securing the United States' technical infrastructure."*

Although the spirit of the strategy is to protect critical infrastructure, while avoiding regulation, there is already a discussion regarding "tying State or Federal funding to IHEs to compliance with certain cybersecurity benchmarks."[1] Although new regulations may not dictate RIT's technology

continued on page 9

In This Issue

Virtual Private Network Installed for Online System Safety

By Cristal Haygood, Project Manager, TSS, cnhits@rit.edu

What is VPN?

VPN is an acronym for **V**irtual **P**rivate **N**etwork. A virtual private network is technology that is used to secure communication between computers across a public network.

The most popular public network is the Internet. Once you send information from your computer to another computer, a packet is created and encrypted so it cannot be read or changed. The packet of information you send, along with millions of other packets, uses the same network resources to send information. Everyone has the same goal in mind, to transmit information from one location to another, without worrying about someone else intercepting it.

A simple example: When you mail a letter, it goes through a process: the mail carrier receives it, a letter is processed through several post offices, and finally delivered to its destination. Once the letter leaves your hand, you hope that the letter is delivered without being damaged or opened. Ideally, it would be great to have the mail carrier deliver your letter directly to its destination instead of going to several locations.

***VPN does exactly that. It creates a secure tunnel for encrypted packets of information to pass through from one computer to another computer*.**

With all of the conveniences of using the Internet for day-to-day functions, it is however, a non-secured environment to pass data, passwords and confidential information through. Many companies have made significant efforts to improve network security so their customers' information is not compromised.

How does VPN help RIT Customers?

Many people access RIT's network from home or other remote locations using a third party Internet Service Provider (ISP) such as RoadRunner, Frontier Link, DSL, or AOL. VPN will allow you to securely connect to the RIT network and access resources.

VPN provides extra security with the following functions: privacy by using encryption and content integrity using authentication. (Authentication ensures that the sender and receiver are indeed, who they say they are.)

continued on page 16

Information Security - Top Down, Bottom Up, and Inside – Out

By Jim Moore, Information Security, jhmfa@rit.edu

If you wonder what is the bottom line, it is about the mission of RIT. Information has long been known to be effective in teaching, learning and research. The Internet, and networking in general have been indescribably valuable in furthering education. But recently, hostility has come to the Internet.

Viruses circulate causing disruption. Unsolicited email is eroding our enthusiasm for communicating in that way. Hostile takeovers of our PCs to become drones in servers in the distribution of illegal content, have caused rebuilds and downtime. Information security is about protection of the mission of RIT through the protection of information resources.

> *"Internet risk continued upwards throughout this reporting period. Internet Security Systems' assessment from the last report indicating that an unprotected computer will be compromised within a day of connection to the Internet remains accurate."* [1]

Computer Emergency Response Team (CERT) reports that Internet attacks have doubled year over year for the last three years, a trend that continued from the early 90's. [2] Internet Security Systems™ reports that the number of vulnerabilities reported rose 65% for the third quarter of 2002 when compared to the same quarter of 2001. [3] In absolute terms, 583 new vulnerabilities were reported in the third quarter of 2002. This translates to 8-9 vulnerabilities per weekday.

In the last year we have seen worms that seek out other hosts to infect, worms that plant backdoors, worms that read your address book and forge addresses to mail their deadly payload on, and viruses that disable personal firewalls. It looks like every year we will have to "re-learn" what information security is all about. But I don't mean to scare you. I mean to recruit you.

You may believe that we are losing the battle right now. This is due to the focus of security efforts being on top down secu-

continued on page 15

EDITORIAL

The Cost of Safeguarding a Network: An Individual and Organizational Effort

By Michelle Cometa macits@rit.edu and Dave Pecora, dlpits@rit.edu

> *"Many IT support providers have the appropriate attitude and aptitude to find a problem and fix it once it occurs. But now we need staff who can understand a complex system well enough to ferret out its weak points and fix them before service is affected. Such highly knowledgeable staff will function as infrastructure managers responsible for the* ***fire proofing*** *rather than the* ***fire fighting*** *– a role shift that is key to the success in the information technology support model." - CAUSE Magazine, "The Crisis in Information Technology Support," p. 15*

The cost to individuals and organizations of safeguarding a network is high and climbing. In light of the increase in use of online capabilities - from multi-function email systems to e-commerce applications - computer use has risen with a correlating rise in cybercrime. Our issue this month focuses on how to keep individual computers safe from hacking as well as safeguarding a vast network that supports the thousands of individuals, departments, applications and resources of RIT. But, what are some of the costs when a computer or network IS compromised?

According to Gartner Research,

> *"Statistics show an alarming rise in cyber-attacks. Since 1998, electronic crime has risen dramatically – 10-fold – according to the latest incident statistics from the Carnegie Mellon Computer Emergency Response Team. In the 2001 Computer Crime and Security Survey, conducted jointly by the Computer Security Institute and the FBI, 85% of respondents said they had detected breaches in their systems during the previous 12 months. Sixty-four percent of them reported financial losses due to those security incidents."*
>
> *Further, the nature of the crimes has changed. According to a study produced by the Computer Security Institute and the FBI, the Internet is a source of frequent attacks: 70% in 2001 compared to 59% in 2000, while at the same time internal attacks dropped from 38% to 31%. Reported average losses from viruses alone, an untargeted nuisance attack were $244 million in 2001 up from just $45 million in 1999."*
>
> Reference: IT Security Breaches are Growing, Gartner Research, January 17, 2002

Cybercrimes cost organizations money, time and effort. To combat this they have installed security officers as the latest trend in new jobs. Organization's also have adopted a variety of policies that show due diligence – that they have taken action to keep its systems safe through monitoring, intervention and security applications such as Virtual Private Networks, firewalls and authentication practices. (*See the VPN article on page 3*)

Weighing security against functionality is a never-ending balancing act. For example, as a consumer, you can order various products from all over the world online. Yet, we are seeing an increase in unwanted marketing via spamming. (*See the Spam article on page 6)* Prospective students can apply to RIT on line as well as send some application payments via electronic means. Yet, we must continually reassure our customers that connecting to our network does not make them vulnerable to access from others who can take identifying information (Social security numbers, banking account numbers, etc.) and use it improperly.

RIT and ITS have made this assurance of safety a core value in all current and emerging electronic applications, and the articles in this issue describe some of the actions individuals can take to support the efforts.

It sounds like a double-edged sword, surely. But with the following daunting statistics about Internet and network growth, we need to have this value of vigilance.

553 million people are now connected to the web from their homes according to a Global Internet trends report from Nielsen/NetRatings.

The United States continues to dominate the Internet population with 166 million users or 30% of the total, followed by Europe with 24%, Asia-Pacific with 14% and Latin America with 3 %. Germany, with 32 million users, the United Kingdom with 29 million and Italy with 22 million, are among the largest non-US markets.

NewsFactor Network, http://www.newsfactor.com/perl/printer/19046

In 2002, roughly 133 million miles of fiber-optic cable stretch under the Atlantic and Pacific Oceans.

continued on page 14

You've Been Hacked!

By Mark Kimble, Manager, Distributed Systems, TSS, mjkits@rit.edu

My primary mission to ITS and thus by reference to RIT is to provide ITS technical support staff with situational awareness of the RIT infrastructure. To do this we have implemented a suite of tools used to monitor networks, servers and applications supported by ITS. This places me at the answer-end of many questions regarding performance and capacity of these systems. Often that question is phrased much like "My network connection is really slow." Notice the lack of question mark in that question?

Frequently complaints of network performance are found to be the result of single computers consuming amazingly high quantities of shared network bandwidth in competition with the complainant's. Often this high consumer's computer is doing so without the owner's knowledge. This usually implies their computer has been hacked and is now sharing copies of software packages or current movies in violation of copyright laws. It is my obligation not to seek these compromised boxes out, but to take action upon discovery. This is a story of a possible scenario such as this:

I called a friend on campus to ask if he was interested in making copies of the new Harry Potter movie he had on his PC for distribution to his peers. He asked what I was talking about in his typically emphatic manner. I broke the news to him; his IP address had just set an all time one-day record for data output to the Internet.

This record would probably not be reported by Warner Brothers as an opening week statistic for their new movie. More emphatic comments flowed from my friend like the bits from his hard drive onto the Internet. I told him I'd stop by and help check out his obviously hacked PC.

As soon as I entered his office I heard the sound of his hard drive thrashing as it expelled data faster than my colleague's flow of expletives. The disk drive activity light flashed in time with the noise.

I snickered and earned more abuse from my friend. He informed me that this PC was less than a month old. How could it have been hacked so quickly? I told him the fresh ones were the easiest; they haven't been secured yet. The vendor ships in a completely hacker-friendly configuration.

He asked how he could have known about this. I ignored his question for the moment and pushed my way into his chair. I took his wonderful multi-button mouse in my carpel-tunnel strained hand and moved the cursor to the "Start" button.

Hack \'hak\ vb : to gain access to a computer illegally.

"Computer security is NOT simple and IS a full-time job."

The cursor lagged, jumped and then flashed to the iconic moniker of all Windows beginnings. I thought for a moment that the hard drive's thrashing might have been rhythmically in sync with the Rolling Stones' "Start Me Up" song now running though my head.

I clicked on the Programs selection and waited as the system paused. I found only four software applications installed since purchase: The Microsoft Office suite, Adobe Acrobat Reader, Corporate Time and AOL Instant Messenger.

A click on the *My Computer* desktop icon confirmed my fear. His brand new computer with a 40-gigabyte hard drive and next-to-no software installed had only five gigabytes of free disk space. I was impressed.

I answered his initial question (*How could it have been hacked so quickly?*) with one of my own, "How could you have NOT known your computer was hacked?" More expletives followed by the more sensible, "No, really. How could I tell?" His asking came as no shock to me as many more technically savvy people than he had been embarrassed by visits from me. I took some time to show him what I'd learned in the first minute at his keyboard.

continued on page 18

Spam: It's Not Just for Breakfast Anymore

By Jason Polito, Systems Administrator, jmpdss@rit.edu

There might be some terminology in the text with which you might not be familiar. If you would like to learn more, I encourage you to visit http://whatis.techtarget.com/. You will find brief descriptions of almost any acronym the IT field throws at you.

ITS new partnership with the Gartner group also provides some excellent content on the subject of spam. The Gartner web site may be accessed through http://www.rit.edu/~wwwits/services/gartner/. You will need to log in with your RIT computer account and password. The article "Why Am I Getting All This Spam," by Joyce Graff is recommended reading.

One of the biggest challenges we face today involves processing the constant presence of new information. Information comes streaming at us from all directions: TV, radio, television, postal mail, web sites, and e-mail. While we may change the channel from Jerry Springer, or turn the dial on the radio, the last two on the list (web sites and e-mail) are the most prone to unwanted solicitation. This article will focus on the abuse of e-mail as a delivery system for unwanted marketing material, or what is better known as Spam.

What is considered Spam?

Spam falls into two categories - solicited and unsolicited. If you sign up for a service or trial through a web site, chances are you were prompted somewhere to signup for a company newsletter or third party offers. Usually such offers are checked by default, so be wary when signing up. Often you can uncheck this box, which will reduce your overall junk mail. If you leave the box checked, your name is placed on a list that is available for purchase.

Herein lies the biggest problem. These lists are available to anyone claiming to be an entity. Companies (and "spammers", as the purveyors of spam are called) will send mail based on these lists, but by law they must offer an "opt out " alternative. Your best defense is to opt out of these mailings.

Legitimate companies will add your name to their own block list, crosscheck it with the purchased master list, and cease sending you e-mail (this can be considered solicited).

Are there laws in place to stop spam?

There are laws from state to state, but mail received in New York could originate from as far away as India. There are calls for international laws regarding spam, but governments are a long way off from reaching the point of actually drafting legislation. California requires that all marketing related e-mail be prefaced by ADV: in the address. This would allow filtering before the mail even entered your inbox. This is problematic:

1. Much mail comes from out-of-state
2. If stopped at the server, it could block legitimate marketing material people wish to view
3. The server is also processing a huge volume of mail that may be unwanted by customers.

What is RIT doing to combat Spam?

When ITS can isolate a piece of mail as spam, it can block it; identification, however, is often difficult. Spam often originates from people abusing ISPs and servers, which are distributed throughout the world. Domains targeted as abusers are banned from honest ISPs, but there is always a new one to take its place. This makes blocking by name very difficult, as it usually changed from ISP to ISP. Sending addresses can also be spoofed, (meaning the name in the FROM area of an email address is NOT actually the sender but the spammer impersonating that sender). Blocking by content could also be difficult as it might filter out much legitimate research information.

ITS is currently looking at solutions that will help reduce the amount of spam. Possible solutions involve products that work in conjunction with our gateways, mail servers, desktop products, and filters. We will give continual updates about solutions to benefit those who are challenged with unwanted spam.

What Is Spam To You, Might Not Be Spam To Me

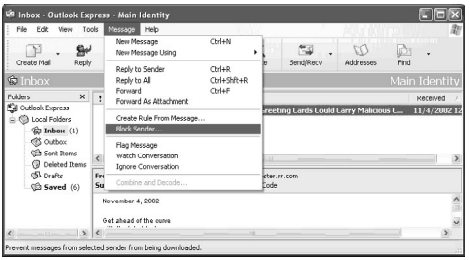
By Jason Polito, Systems Administrator, jmpdss@rit.edu

The individual e-mail that creeps into our mailboxes can sometimes be annoying. Yet, blocking all unsolicited email from entering the RIT network may not be appropriate as some people wish to receive certain items. The solution likely exists in your current e-mail program.

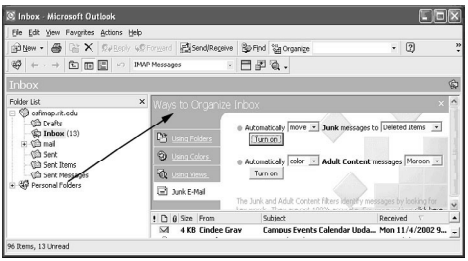
Most of the mail clients used on campus have filtering options built in, but require effort on the end users part. Maintaining filters and blocking unwanted messages is an ongoing task as new addresses and mailings propagate the Internet. There are things available to you on your own desktop to combat spam.

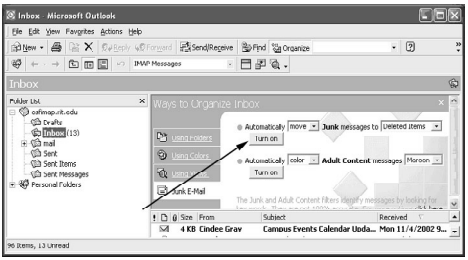
How do I block these e-mails from my e-mail client?

For those using **Outlook Express**:



1. Highlight the message considered junk mail/spam
2. From the Message menu at the top, select "Block Sender"
3. All mail from this address is removed from your inbox from this point forward.





For those using **Outlook 2000/2002**:

1. From the "Tools" menu, select "Organize"
2. A menu appears above your e-mail titled "Ways to Organize Inbox"
3. From the available menu, click on "Junk E-mail"
4. Select the actions you wish to occur when this mail arrives.
5. You can highlight the junk mail a separate color from other mail, or move it to a different folder for removal or perusal at a later time.
6. Select "Turn On" and close the menu using the "X" in the left corner of the menu
7. Now that the filter is activated, right mouse click on the message considered Junk mail/ spam
8. Select "Add to Junk senders list" from the available menu
9. Any mail from the address specified is now processed by your chosen junk mail options.

continued on page 12

ITS News

Vini, Vidi, Viri (I Came, I Saw, I Infected)

By Dave Bradstreet, Residential Computing Administrator dmbdss@rit.edu, and Jeremy Beyette, Residential Computing Consultant

Many of the computer viruses today fall under the category of **Worms**. A worm attempts to replicate itself through open network shares or by e-mailing itself to e-mail addresses found in the address book of a computer. Some of the subtle things worms do is open up your computer ports and allow access by the worm's sender to access and sometimes remove files from your computer or, in some instances, delete information and data saved on your various drives.

There were two large-scale viruses released toward the end of September, *Bugbear* and *Opaserv*. Bugbear is a mass-mailing worm that:

- Stops anti-virus and firewall processes.
- E-mails itself to everyone in an address book with its own messaging engine.
- Creates a backdoor for intercepting keystrokes and allows remote administration.
- Replicates itself to other computers through open network shares.

Opaserv is a worm that attempts to replicate itself to other computers through open network shares. If it finds an open network share, it copies itself to that computer in a file named **Scrsvr.exe** and then attempts to download updates from www.opasoft.com.

There are steps that you can take to help protect yourself from existing and new viruses

Other viruses that remain on the list of top threats and that are often discovered on the RIT network include *Klez* and *Nimda*. Klez is a mass-mailing worm that attempts to copy itself to open network shares, e-mail itself to entries in a Microsoft Outlook address book, and cause files to become zero bytes in size on several days during the year. Nimda is another mass-mailing worm that sends itself out by e-mail, replicates through open network shares, copies itself to vulnerable Microsoft IIS web servers, and infects files on local and remote computers.

There are steps that you can take to help protect yourself from existing and new viruses.

- **Use anti-virus software**. McAfee VirusScan is available for free to all RIT students, staff, and faculty. The file can be found at http://www.rit.edu/~wwwits/services/security/.
- **Update your anti-virus product on a regular basis**. Most antivirus products feature automatic or scheduled update capabilities to keep you protected from the latest threats.
- **Practice e-mail safety**. Microsoft Outlook is a feature rich e-mail client, but is also the target of many attacks. To prevent these attacks, follow several steps to prevent infection:

    1. Delete e-mail from unrecognized senders
    2. Turn off the preview pane
    3. Do not open suspicious or unrecognized attachments
    4. Last, install updates regularly

Installing Windows and Office updates on a regular basis help close security holes and prevent infection from a virus. Windows Updates can be found at http://windowsupdate.microsoft.com/ and Office Updates can be found at http://office.microsoft.com/.

Need Help With Viruses?
Contact the ITS Help Desk to answer any questions about computer viruses and installing virus programs for your computer. Call the HelpDesk at 5-HELP (4357) or 5-2810 TTY.

Balancing Intellectual Freedom, Privacy and Security

continued from page 2

security plans, the reality of funding may drive it instead.

In addition to the Strategy, EDUCAUSE has submitted a contribution on behalf of the higher education community. The EDUCAUSE document contains more detail and begins to address the problem of how to strike a balance between intellectual freedom, privacy and security.

They believe that this balance can be achieved in three areas:

- The administrative level (policy),
- The user level (education), and
- The technical level (best practices and specific security technologies).

ITS supports this belief, and asks for the RIT community's support in this balanced approach. ITS is continually working with the Information Security Officer, under Risk Management, to provide input and support in providing policy and education to the RIT community.

What is ITS doing to provide a higher level of security?
Although ITS and Risk Management have not completed a formal security strategy, ITS has begun to tighten security and provide alternatives to leaving systems and portions of the Campus Network open to the Internet. These alternatives include:

- **Virtual Private Network (VPN) -** provides a secure connection to the Campus Network from off-campus
- **Firewall technologies** – ITS is currently supporting some departmental firewall solutions and is partnering with the Golisano College of Computing and Information Sciences to pilot advanced functionality.
- **Port blocking at the Internet border** – this method is utilized to block specific TCP/IP ports (system-to-system communication avenues) that are known to be security threats
- **Packet filtering/prioritization** – allows for legitimate network traffic to have priority over peer-to-peer traffic generated by sharing of music, movies, etc.

What can you do to help?
Educate yourself on the fundamentals of security based on your level of involvement in computing systems. As an end user, you can play a significant role in securing our environment by securing your own desktop PC.

Methods of securing your desktop include using strong passwords and keeping up to date with operating system patches and upgrades. If you would like to learn more about securing your desktop and the environment around you, please contact your ITS customer support representative. To learn more on-line, check the following resources referred to in this article as a starting point. Contact ITS at helpdesk@rit.edu for additional resources or with questions.

Footnote:
[1]From "The National Strategy to Securing Cyberspace" draft, page 34

Resources:
"The National Strategy to Secure Cyberspace" draft, submitted by The President's Critical Infrastructure Protection Board, http://www.whitehouse.gov/pcipb/
"Higher Education Contribution to National Strategy to Secure Cyberspace", submitted by the staff of EDUCAUSE, http://www.educause.edu/security/

The Critical Infrastructure Protection Board report can be found at the following site:
http://www.whitehouse.gov/pcipb

This page opens to a White House news release giving readers background about the initiative then the option to download the draft report in HTML or PDF versions. From the news release, "*President Bush directed the development of a National Strategy to Secure Cyberspace to ensure that America has a clear roadmap to protect a part of its infrastructure so essential to our way of life. The draft of that roadmap was developed in close collaboration with key sectors of the economy that rely on cyberspace, State and local governments, colleges and universities, and concerned organizations.*"

Privileges and Responsibilities Defined in the Computer Code of Conduct

Code recognizes that simple actions often affect more than the individual

By Donna Cullen, HelpDesk Lead, dccacc@rit.edu

> *All I am saying is simply this: In a real sense all life is inter-related. All persons are caught in an inescapable network of mutuality, tied in a single garment of destiny. Whatever affects one directly, affects all indirectly.*
> Martin Luther King Jr., Mankato Minnesota, November 12, 1961

Martin Luther King used these words to express what it is to be a member of a society. Each time you or I use the RIT network, we are "in an inescapable network of mutuality…whatever affects one directly, affects us all indirectly." Not only do our actions on a connected computer impact people connected to the RIT network, but also there is the potential for our actions to impact anyone connected to the Internet. We become part of the global community.

It is in the spirit of a global community that RIT developed the *RIT Code of Conduct for Computer and Network Use*. In addition to providing definitions for the terms used in the policy, the Code provides you with information on what you can expect and what RIT expects of you when you use the RIT network systems.

Relationship to Other Institute Policies

Much of what you do on the computer has a counterpart in other actions you take. For example, an email message to a student is similar to a handwritten or typed memo. This section of the Code relates your computer use to behaviors covered by other campus policies. Respect for privacy is outlined in RIT's *Policy on Privacy*. RIT's *Policy Prohibiting Discrimination and Harassment* covers harassment through the use of the computer network. There are a number of other campus-wide policies and department policies that could impact your use of the RIT network.

continued on page 17

Law Officials Involved in Some Computer Crime Cases

By Donna Cullen, HelpDesk Lead, dccacc@rit.edu

Joey is typing an essay on popular culture for his English Comp class when a knock sounds on the door of his RIT apartment. "Yeah, it's open," he mumbles as he clicks on his spellchecker. The knock comes again. Disgusted, Joey yanks open the door while still facing his computer screen.

"Mr. Nosnum, Joseph Nosnum?" a deep voice asks.

Annoyed, Joey barks "Yeah?" But when he turns around to see a man and a woman dressed in suits, he blurts "I mean yes ma'am, yes sir."

"Mr. Nosnum, we are FBI agents…" Joey fails to hear much after "FBI" as his attention turns to the badges being flashed in his face. His thoughts are on his parents and how to explain a visit by the FBI. The legalese the officers are sharing is about him being a suspect in a computer software trafficking ring case.

True story? No. Stuff only seen on TV crime shows? Not quite. Incidents very similar to this have occurred on the RIT campus.

When outside law officials are involved, the investigation starts with Campus Safety receiving a subpoena. Campus Safety contacts departments on campus to gather relevant data. In the case of computer, network or telecommunication issues, ITS is also contacted. In the course of the investigation, property including a personal computer or storage media may be confiscated by law enforcement.

Fortunately, the misuse of RIT computer, telecommunications or network resources is seldom the makings of TV drama. Most incidents are processed without the involvement of outside law enforcement agencies. RIT does, nevertheless treat all misuse seriously.

Investigations typically begin with a complaint. Some complaints are from a member of the RIT community. Other complaints are initiated off campus. External complaints include site managers noticing an RIT machine scanning ports and firms hired by the recording, movie and software industries reporting the illegal sharing of copyrighted material.

continued on page 18

What is the Least That I Can Do To Secure My Computer?

By Dave Bradstreet, Residential Computing Supervisor, dmbdss@rit.edu

Many times we are asked, "What can I do to keep my computer secure that won't take the entire day?" Here are a few things that you can do to protect your computer and, more importantly, your information.

Keep Your Operating System Up-to-Date

Apple and Microsoft often release patches for security holes found in their operating systems (yes, security holes are found regularly). If you do not take steps to fix these holes, Internet 'hackers' can take advantage to gain control of your computer.

Microsoft: <http://windowsupdate.microsoft.com>
You can always access this in Windows from Internet Explorer -> Tools menu -> Windows Update.
Apple: <http://www.info.apple.com/support/downloads.html>
This can be accessed from Control Panels (OS 9) or System Preferences (OS X) -> Software Update.

Keep an Administrator Password in Microsoft Windows 2000/XP and Mac OS X

Windows 2000, XP, and Mac OS X are multi-user operating systems. That means that multiple people can use the same computer and have their own files stored on it. It also means that one person (you) must administer the system. This is true even if you are the only user. The ability for multiple people to use the computer is always there.

Microsoft:
Start -> Settings -> Control Panels -> Users and Passwords (2000) or User Accounts (XP)
Windows 2000
- Double click on the Administrator User
- Enter a new password

Windows XP
- Choose the Administrator account
- Choose Create Password
- Enter a new password

Mac OS X:
System Preferences -> Accounts
Select your account and click Edit
Enter a password (if none exists)
You may also want to uncheck the Automatic Login option. This will prevent anyone from walking up to your computer and using it without your permission.

Keep an UPDATED Virus Scanner on Your Computer

Many computers have a virus scanner installed. Unfortunately not everyone updates the virus definitions file. This is the file that tells the scanner what all the newest virus's are. An updated scanner will alert you when a potentially threatening file is being downloaded onto your computer. It can also detect other types of problems such as Backdoor IRC Trojans, Spy-ware/Ad-ware, and future virus's.

You must update your virus scanner regularly, about once a week. This way, your computer will never be surprised by a new virus. Without these updates your virus scanner is WORTHLESS.

RIT provides all members of the community with a FREE virus scanner. You can find information and downloads at <http://www.rit.edu/~wwwits/services/security/>.

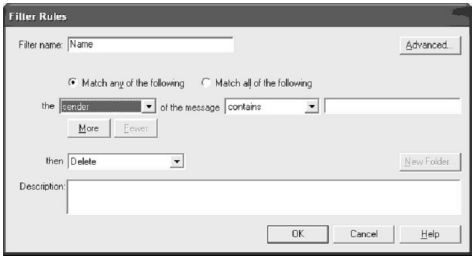
Microsoft provides updates and patches to Microsoft Office. You can find more information at the following addresses:
Windows: <http://office.microsoft.com/>
Mac OS: <http://www.microsoft.com/mac/>

What Is Spam To You, Might Not Be Spam To Me

continued from page 7

For those using **Netscape 4.7**:

1. From the "Edit" menu, select "Message Filters"
2. Select "New"
3. In the available box, name the filter, and set the actions.



Configuring these settings can be a bit daunting. Improper configuration of filters can block whole domains such as yahoo.com, aol.com, or hotmail.com, which could block legitimate e-mail. Contact the ITS HelpDesk at 5-4357 or 5-2810 (TTY) for help if needed.

Are there other options?

There are many desktop products, but they work much like the built in features of your e-mail program. The built in features of your client, and the desktop solutions require a great deal of input from the user, and are not 100% effective. The steps involve identifying spam, and setting filters accordingly (much like in the above built-in filters).

You *must* perform the filtering operation, because you know what you consider "spam." Once these initial filters are setup, the program runs in the background. Due to the changing addresses of spam, continual updating is necessary for the products to be effective.

To alleviate this constant need for setting filters, companies such as McAfee are providing services, which update spam addresses, much like a virus program updates virus definition files. The program downloads an updated spammers list daily (blacklist), which removes the burden of setting filters manually. There is a catch, however. These blacklists are not tightly controlled by any one entity or government group. In the past several legitimate companies and colleges have found themselves on these blacklists, causing their e-mail to be bounced back or even deleted.

Unfortunately, none of these desktop products are 100% effective. Many only work with specific types of mailboxes. Two popular products, Spam Buster and Spam Killer, work only with the POP protocol (most people at RIT use IMAP protocol servers).

A more drastic method is to use what is known as a DEA (disposable email addresses). These software programs generate false e-mail addresses when you are browsing various sights and signing up for their services. The advantage to using a DEA is that it can pinpoint who is selling or harvesting your information. You can then send this information to various organizations that work to better existing practices or put them out of business all together. One such sight is http://www.spamcon.org.

So what is the solution?

There is no one solution for spam. And because spam is not the same to everyone, stopping it completely is not a likely outcome. It has joined the ranks of telemarketing, and postal mail as a mainstay of commerce. The low cost, and anonymity of e-mail makes it that much more appealing to marketers. Your best defense currently is to use your built in email client filters, and add mail filters as it comes into your inbox.

ITS will continue to evaluate products, and inform the campus of its findings and recommendations.

If you are interested in exploring a third party solution, the following sites might prove helpful.

http://spam.abuse.net
http://www.elsop.com/wrc/complain.htm
http://spamcop.net
http://www.mcafee.com

Your best option is to block the e-mail you do not wish to receive. If you continue to receive these e-mails after 4-5 days, report the incident to abuse@rit.edu. Include a copy of the e-mail, and the steps you have taken thus far to stop receiving the mail. Good luck and happy hunting.

Passwords and Patches: Updating and Protecting your Computer

Jason Polito, ITS Customer Support, jmpdss@rit.edu and
Vince Incardona, ITS Customer Support, vxiacc@rit.edu

In all operating systems (OS), programmers and users alike find problems that inhibit productivity and compromise security. Fixes, patches, and add-on programs seek to address these issues. Typically, these patches are applied by one's friendly neighborhood administrator with a quick, but polite, "I just need to install a quick fix. It'll only take a minute."

However, the power to do this, for both PC and Mac users, is at your fingertips. Microsoft has a very useful website that scans your PC and recommends particular updates or enhancements. These updates can then be downloaded and installed with a minimum of effort. Likewise, Macintosh offers a similar method of OS protection, more often an enhancement, which is embedded in the OS.

It is important to apply these updates, for more often than not, they address security issues. Weekly, people are finding security loopholes in software packages that have the potential to compromise a user's computer. Security risks are found daily on many operating systems. Visit <http://www.securityfocus.com/> for information regarding software security.

Microsoft has been in the news quite a bit lately because of the security holes discovered in their programs. The company has stepped up to the challenge and offered fixes within a matter of days, and sometimes hours. (You may have even heard of Bill Gates' interoffice memo titled, "Trustworthy Computing." If interested in reading it, go to <http://news.com.com/2009-1001-817210.html>. It says, basically, that the company plans to make security a #1 priority in future products.)

A majority of these OS exploits (and it's not just Microsoft) are found by security corporations, consultants, and concerned professionals (often alerting the companies to the problem before announcing them publicly) and are only truly dangerous in the hands of experts who understand the ins and outs of various programming languages. This limits the field of abusers to a select group of people The problem is that attaching an unsecured computer to the Internet makes it accessible it to anyone out there in cyberspace with the knowledge, skill and inclination to attack your machine.

This article was first published in ITS News May 2002; we thought the information is as timely now as it was then and worthy of repeating in our security issue. –eds.

Use Strong Passwords

Your first line of defense, therefore, should be a set of strong passwords. When choosing passwords, it is important to understand that you are using them to protect your machine from attack by other machines, as well as by attack from humans. A password protects a machine by not allowing access to it until the correct combination of figures is supplied. A human can manage to type sixty or seventy words a minute if they're really good, and without some method to rule out all but the most likely keywords, it could take a lifetime to actually hit on the right password.

However, a computer's utility lies in its ability to systematically perform those operations at nearly the speed of light. This means that someone trying to execute a dictionary attack on your password by using a typical off-the-shelf Pentium computer to try all possible English words is likely to get through in less than a minute if you use a password that can be found in a standard English dictionary. If you use a password that isn't in the dictionary, but consists only of lowercase alphabetic characters, that same Pentium computer can crack that password inside of an hour if it's six characters or less in length.

A person who knows you well enough to know the names of your spouse, children, dog and favorite vacation spot can be into your machine in less time than that just by guessing what you would choose as a password. This is why it's important to make sure that every account on your machine is protected by a strong password. *A strong password is one that is obscure enough that people cannot easily guess it, and it is also complex enough that a machine cannot randomly discover it during a brute-force attack.* Current research[1] has shown that in order to protect against such an attack, a password should:

- Be at least eight characters in length
- Contain both upper and lowercase characters
- Contain both digits and alphabetic characters

The aforementioned research shows that the same Pentium computer which could crack a dictionary password in less than a minute would take over 16 years to crack a password

continued on page 14

Passwords and Patches: Updating and Protecting your Computer

continued from page 13

that met the above criteria. Also, remember that there may be more accounts than the one you use every day – many people forget about the account called "administrator" when setting passwords, and this is the most powerful account on the machine.

How to perform software updates.
Before proceeding with any of the following steps, it is recommended that no other applications are running. Also, do not begin another process during the updates, and save all existing work before installing the updates, as the computer will most likely require restarting. Backing up all of your personal and business files is also recommended. However, ITS recommends having a backup of these files ALL of the time, not just before performing updates. A zip-disk, CD-burner, or network share make for excellent backup media. If you have never copied your files to media of this type, or if it has been a while, you should make it a priority!

If you are a **Macintosh OS 9.2** and below user, simply click on the rainbow colored apple menu in the top left hand corner, scroll down the list to "Control Panel" and select "Software Update." This can be scheduled to run automatically by selecting the "Schedule" button in the Software Update window. If you do not wish to have software automatically updated, select the "Update Now" button. A list of available updates is shown. From here, you can select the desired updates and install them.

For **Macintosh OS X** users, click on the Apple menu located in the top left-hand corner. Scroll down to "System Preferences." From the system preferences window, select "Software Update" located towards the bottom. Again, you have the option to automatically schedule updates. If not, select the "Update Now" button. You will be presented with a list of available updates from which you can choose.

If you use any version of **MS Windows**, there are two methods. The easiest is to open Internet Explorer. Select the "Tools" menu, and click on "Windows Update." This will take you to the Microsoft Windows Update home page. Likewise, you can get there by typing <http://windowsupdate.microsoft.com> into the address bar of Internet Explorer (*Note: Netscape does not automatically scan for updates, so we recommend using Internet Explorer for performing updates).*

Once there, click on "Product Updates." If you have never run an update, windows will ask if it is OK to install the Critical Update Scanning feature. Select "Yes," or "OK." Once the applet is installed, the windows update page will show a list of available updates. Be sure to install anything listed under the "Critical Updates" section. These are the most important for security and operability.

Scan for updates at least weekly. If you have never been to either Apple's or Microsoft's sites, you may have to visit them several times to install all updates since a reboot is often required after each individual install. However, the peace of mind will be worth the added hassle of shutting down and starting up. As always, the ITS HelpDesk is available for questions and assistance.

The Cost of Safeguarding a Network

continued from page 4

Since 1998, capacity on Trans-Atlantic and Trans-Pacific cable has grown more than 20-fold according to TeleGeography Inc, a Washington-based firm that tracks international telecommunications.

Global Internet Use, Rochester Business Journal, Special report, May 24, 2002

An IT organization is only as strong as its people who know the technology well. In an effort to change with the trends in the IT field, from "fire fighting" to "fire proofing", the ITS organization has made more than best efforts to maintain the integrity of a system that we at RIT use every single day.

Enjoy the articles. We hope that they are useful and helpful in your efforts to keep your systems safe. Our staff is available to assist in your efforts. We welcome your feedback about the articles and can be reached at dlpits@rit.edu and macits@rit.edu.

Information Security - Top Down, Bottom Up, and Inside – Out

continued from page 3

rity, which is largely out of sight of the end user. You see the attacks that succeed, but you don't see even more attacks that fail.

The top down security strategy is where the most valuable data is collected in a few select places, then is heavily defended. In essence it's a "bank vault strategy" and a good one to employ. And we, as an Institute, intend to get better at it. We will do this by better identifying what data is valuable or confidential. We also need to agree on how we handle and communicate confidential or valuable data. We can technically update our top down security too.

> "You see the attacks that succeed, but you don't see even more attacks that fail."

Bottom up, really is talking about the desktop. PC stands for personal computers. That is where we work. As the word "personal" suggests, that is where the data that is valuable to us is prepared and stored. Bottom up approaches address personal productivity as well as personal confidentiality.

For some time, I have been looking at the area of Personal Information Assurance. I have also been watching our culture. A few years ago people questioned the value of anti-virus software. Today, these questions center around how often should anti-virus signatures be updated, with the most common response being "Daily."

With Internet service providers such as Roadrunner™ and DSL, personal firewalls are common. Culture is changing. As culture goes digital, bottom up security is gaining importance. That is good. Individuals have a greater sense of the value of their own data and documents. So bottom-up security will involve awareness, training, events and even some new products. This is where we look forward to getting your input, and your support.

Inside – Out Security is really just talking about better use of inside and outside resources for both top down and bottom up security. Inside RIT security initiatives are popping up all over. ITS is sharing its directions in this Issue. Faculty in the College of Liberal Arts, Golisano College of Computing and Information Sciences, and the College of Applied Science and Technology have been sending information my way about courses they are teaching and research they are doing. Groups on campus are documenting and publishing best practices and beginning to get the recognition that they deserve.

And I can't say enough about RIT's students. I have had the privilege of working with a number of co-op students, and I am amazed. The student workers have done research on operating system configuration baselines, strategies for combating programs that log keystrokes (and capture passwords), and extended existing public domain security tools. Some of the work the students have done has also been volunteer time. In addition, some of the security awareness documentation is documentation that students have written to share with other students. The student clubs on campus in computer science, IT, and security are all a source of inspiration, as security is fully integrated in what they do.

Outside security resources is a developing area. RIT became the first educational member of the Rochester Area Information Security Forum (RAISF). It is continuing with partnerships with other security organizations such as the Forum of Incident Response and Security Teams (FIRST), and the Center for Internet Security. We are also working with other universities on various security-related projects. We are collaborating with Purdue University on handling computer incidents, and with Yale University on incident investigations.

It is an exciting time to be at RIT. We are at the forefront of cultural change. And will ride the wave into a better, more productive environment.

Modifying the expression slightly, "*It is a big job, so everybody's got to do it.*"

References:
[1] *ISS Internet Risk Impact Summary: March 26, 2002 through June 24, 2002*. (June 24 2002), Retrieved July 1, 2002, from Internet Security Systems website: https://gtoc.iss.net/documents/summaryreport.pdf
[2] *CERT/CC Statistics 1988-2002*. (October 4, 2002), Retrieved November 1, 2002, from Computer Emergency Response Team / Coordination Center , Software Engineering Institute, Carnegie-Mellon University website: http://www.cert.org/stats/cert_stats.html
[3] *ISS Internet Risk Impact Summary: June 25,2002-Sept 27, 2002*. (September 27, 2002), Retrieved November 1, 2002, from Internet Security Systems website: https://gtoc.iss.net/documents/summaryreport.pdf

Virtual Private Network Installed

continued from page 3

What will I see when I connect to VPN?

You will not see:

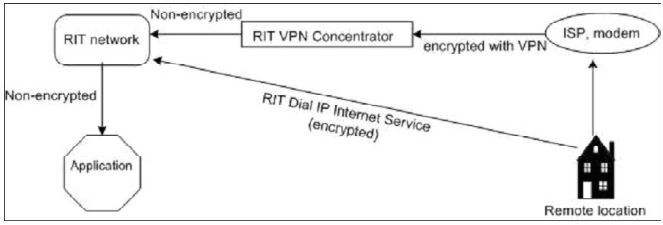
- The same desktop (background picture and shortcuts) if you use a computer other than your desktop computer at work.

You will see:

- For Windows - a padlock in the task bar which will remain until you have disconnected from VPN
- For Mac- a blue dot next to an active connection in the VPN Client application window.
- You will see the desktop settings of the computer you are using.

When should I use VPN?

Use VPN to access RIT's network if you use a third party ISP from your remote location. From this location to RIT, a connection is made to RIT's VPN concentrator. The concentrator is a device that allows the connection to continue to RIT's network. Once you are connected to the network, it terminates the connection that was created from the remote location to the concentrator.



You do not have to use VPN if you use RIT's DialIP Service because it creates the secure connection needed to access the network. No matter how you connect to RIT's network, the level of security inside the network depends upon the security of the application. If you are accessing an application that requires you to log in, that application has a higher level of security as opposed to an application that does not require you to log in.

For more information about VPN, contact the staff at the ITS HelpDesk at helpdesk@rit.edu

In addition, information can be found on the ITS Web page at: http://www.rit.edu/its/services/vpn

Safeguarding Your Computer…We Have Ways…
The staff of the ITS Help Desk and Distributed Support Services (ITS representatives based in colleges providing desktop support) are available to answer any questions about safeguarding your computer. Contact them through the HelpDesk at 5-HELP (4357) or 5-2810 TTY.

Computer Code of Conduct

continued from page 10

User Privileges and Responsibilities

RIT policies not only govern what you do while part of the RIT community, they also provide you with guidelines about how you can expect others to treat you (and your computer). The Code and associated policies provide you with some freedoms. Balanced with these freedoms is an expectation that your actions do not limit or impose on the freedoms of others or the performance of the RIT systems.

Responsible Use of Resources

In exchange for the privileges associated with membership in the RIT computing community, users assume the responsibility to use the community's resources in a responsible and professional manner. This section of the Code expands on this concept to outline specific activities you are expected to carry out and some you are expected to avoid.

RIT Rights

RIT system administrators, in performance of their duties as stewards of RIT computer and network resources, require a higher level of access to the RIT network and resources. This section outlines under what conditions these privileges are used.

Reporting, Investigations, and Sanctions

The *RIT Code of Conduct for Computer and Network Use* is most effective when each member of the community assumes the responsibility to be alert to and report violations. Expected violations of the *RIT Code of Conduct for Computer and Network Use* should be reported to the email address abuse@rit.edu. The reports are received by ITS staff and are distributed as needed to the appropriate administrators on or off campus. For example, an abuse report citing a violation that concerns a person using *Yahoo,* would be referred to the support staff at *Yahoo.*

There are many campus agents that are associated with investigations. Agents include local system administrators, Residence Life staff members, Campus Safety officers and Judicial Affairs. In addition, off-campus agencies or law officials sometimes start investigations.

"The Code and associated policies provide you with some freedoms. Balanced with these freedoms is an expectation that your actions do not limit or impose on the freedoms of others or the performance of the RIT systems."

Sanctions are sometimes considered an appropriate response due to the severity of the impact of the violation. The security or stability of the RIT or an external network can also indicate temporary or longer term sanctions in response to the violation.

Process

A group comprised of representatives from across the Institute developed the *RIT Code of Conduct for Computer and Network Use.* The group consulted policies adopted at other institutions in an effort to keep current with the "global community" and to ensure the appropriateness of RIT's policies. The policy was then shared with the student, faculty and staff governance groups on campus–these groups all approved the current policy.

As a member of the RIT community, it is hoped that you consider the *RIT Code of Conduct for Computer and Network Use* a helpful tool. Should you have any questions about the policy or need an interpretation of the policy for a specific case, the staff is prepared to assist you. Contact the ITS HelpDesk at 5-HELP (4357) or 5-2810 TTY with your questions.

The Code of Conduct for Computer and Network Use can be found at:
http://www.rit.edu/computerconduct

Any suspected violations of the Code of Conduct can be sent to:
abuse@rit.edu

You've Been Hacked!

continued from page 5

First, I said "Hacked computers don't announce in an AOL-style voice over their speaker 'You've been hacked!' So I'll give you a break. But the clues are right here." I was sure I impressed him with my imitation of the AOL voice but he seemed unmoved. "Look at the disk drive activity light and listen to that thing thrash. You're not even using the computer and the thing is very busy. See how the mouse moves – jerk lunge jump? Something is eating CPU processor power. And lastly, your hard drive is full and you've put nothing on it yet." My friend looked stunned.

I told him the grim truth, "Computer security is *not* simple and *is* a full time job. Entire companies, organizations and even job positions here on campus have been created for the purpose of managing computer security. Although there is no single indicator that proves you have a hacked computer there are some good, albeit fairly subjective, symptoms that may indicate the need for technical intervention:

- A rapid and unexplained decrease in available hard drive space. (Although you could just need some hard drive cleanup.)
- A constantly thrashing hard drive. The constant noise or flashing activity light could indicate someone else is using your system. (But it could also indicate your system needs a tune up.)
- Slow or jerky mouse movement. If the mouse is normally a smooth mover and suddenly the mouse is slow, it might be time to have it checked.
- Significantly slowed application start up.
- A phone call from ITS indicating you've been hacked. Though ITS does not monitor user network usage, the top consumers of network bandwidth have been found more often than not, to be hacked. Additionally as the registered point of contact for the rit.edu name space, RIT receives email from the world on systems with our IPs involved in suspicious activity.

What does it mean if a computer has been 'hacked into'?
If your computer has been "hacked" into, someone has gained access to your computer without your permission and/or knowledge. If your computer is hacked into, any private information you have can be shared, others can perform illegal activities through your computer (leaving you responsible), AND there's the possibility of LOSING all your data and programs.
http://resnet.rit.edu/modules

I stood, reached down behind the computer and pulled the network cable from the wall jack. I told him that ITS has people that have become, sadly, overly experienced in cleaning up after such invasions and that I would send someone over to help him plug his PC back in. He mumbled something relating a particular pack animal and intelligence, but I missed it as I was singing "Start Me Up" out loud as I returned to my office.

Law Officials Involved in Some Computer Crime Cases

continued from page 10

The roles ITS takes are investigative, protective, educational and to provide assistance. ITS isolates the person responsible for the involved machine. If the performance or security of the RIT network is in jeopardy, the machine is isolated from the RIT network.

ITS provides information on the proper use of the RIT network. Staff assists in setting up the machine with virus protection and operating system patches. Some complaints are referred to Campus Safety for further investigation and referral to the RIT judicial process.

RIT guidelines for use of computer, network and telecommunication resources are outlined in the *RIT Code of Conduct for Computer and Network Use*. Violations of the code can result in sanctions.

The departments associated with the RIT judicial process levy sanctions. Denial or restricted access to ITS managed resources is sometimes a part of the sanction. In such cases, ITS restricts or enables resources based on directives from the judicial departments.

MacCareful

By Donna Cullen, HelpDesk Lead, dccacc@rit.edu

Hackers, worms and viruses made Windows and Linux the most vulnerable operating systems in 2002. Macintosh systems were among the least prone to attack according to a risk management report issued by mi2g Ltd. mi2g reports that only about 2% of the vulnerabilities appearing in the first 10 months of 2002 were associated with the Mac OS. In contrast, Windows accounts for over 40% and Linux for nearly 20% of the application, server software and operating system vulnerabilities. (See http://www.mi2g.com/ for more information.)

Does this mean that if you own a Macintosh, you do not need to worry about your system being compromised? Or your best protection against a compromised machine is to pack up your Windows or Linux machine and head for the nearest Apple retailer? The most reasonable answer to both these questions is no.

A virus, worm or hacker attack is inconvenient and costly enough that even the least vulnerable computer should have simple measures applied. The "Classic" Mac operating systems have proven to have a low rate of vulnerabilty. Mac OS X, a version of the Unix operating system, is vulnerable to any potential Unix-based security risks. However, the vulnerabilities currently associated with Unix are minimal.

One of the simplest and most effective protective actions is to install and update virus protection software. Members of the RIT community can download and install Virex for their Macinstosh. See http://www.rit.edu/its/services/security/ for download, installation and configuration information. For RIT-owned computers on campus, ITS staff can assist you in downloading and configuring the software.

System administrators for Macintosh servers as well as individual users might want to consider investigating firewall software. ITS does not currently recommend a firewall for Macintosh systems but we are willing to work with you should you consider a firewall necessary. Firewall technology for the entire RIT campus network is part of a current ITS project.

Contact the ITS HelpDesk if you have questions about installing or evaluating software for protecting your Macintosh system. It is never too early to be MacCareful!

Check Closings with Campus Cancellations Hotline

With winter here, campus closings are a strong possibility. To ensure that our students, faculty and staff know of closings, an automated call line provides information about cancelled day, evening and weekend classes or special events due to weather conditions or other emergencies. To access this line, dial:

475-7075 (voice) 475-7076 (TTY)

Please share this information with your co-workers and student workers. It may save them a trip to campus while we are in the throes of one of our infamous Rochester snow storms!

ITS Update

New RIT Messenger Subscribers: Training sessions

Voice/TTY messaging training sessions continue this fall for all new on-campus users. The following is a list of November training sessions available for new faculty and staff.

Date	Voice Mailbox	Dual Language Mailbox*
Dec. 3	10 a.m.	11 a.m.
Dec. 11	2 p.m.	3 p.m.
Dec. 19	10 a.m.	11 a.m.
Dec. 23	10 a.m.	11 a.m.

**Dual language mailboxes can accept voice and TTY messages*

Classes will be held in building 99, room 1285
Please call Char Ipacs at 5-5858 to register for training.

ITS Contact Information

DSS Computing Labs

Hours, locations, hardware, software, and reservations information available on the web at:
http://www.rit.edu/its/services/computer_labs

Telecommunications Services

Located in the Facilities Management building (99)
To contact the Telecommunications Services call 475-5800.

ITS HelpDesk

Located in the Gannett building, rm. 7B-1113

To contact the ITS HelpDesk

- Call 475-HELP or 475-2810 (TTY)
- Send e-mail to helpdesk@rit.edu

Regular hours

Sunday	12 p.m.–6 p.m.
Monday–Thursday	8 a.m.–8 p.m.
Friday	8 a.m.–5 p.m.

ITS News is published monthly, September–May, for RIT students, faculty, and staff. It is available in electronic form through the World Wide Web at http://www.rit.edu/ITS

ITS News is created with AdobePageMaker 6.5 on a Dell OptiPlex GX1 and is printed at a service bureau through RIT's HUB. Photographs taken with Nikon COOLPIX 900 digital camera.

Managing Editor: Dave Pecora, dlpits@rit.edu

Editor: Michelle Cometa, macits@rit.edu

Design/Layout: Omar Phillips, odphelp@rit.edu

ITS News is printed on Graphica Smooth Cool PC White recycled paper and is itself recyclable.

Rochester Institute of Technology
Information & Technology Services
135 Lomb Memorial Drive
Rochester, NY 14623-5608