

IRM NEWS

JANUARY 2006

INSIDE THIS ISSUE:

CYBER SECURITY AWARENESS	1
FIREWALLS	1
COMPUTER VIRUSES	2
POP-UPS AND POP-UP BLOCKER	2
ALL ABOUT SPAM	3
YOUR AOL ACCOUNT AND FAU E-MAIL	4
PASSWORDS	4
SPYWARE	5

TO KEEP YOUR COMPUTER SE- CURE:

- Use password-protected screen savers (on a PC, go to Start -> Control Panel -> Display; select the Screen Saver tab, and check the box for "On resume password protect").
- When you leave your desk, lock your computer (ctrl-alt-del) or logoff so it is protected by your password when you are away
- Do not place your password on a sticky-note taped to your monitor, under your keyboard, or in your desk
- Do not share your password

CYBER SECURITY AWARENESS

The focus of this issue of IRM News is on computer security and ways that you can protect your computer and your information.

Computer security must be followed on many levels:

- Network security via authentication practices, firewalls, virus scanning
- Desktop computer security, again with good authentication practices, personal firewall, but also file backups, virus and spyware detection software
- Personal security, protecting your personal information, backing up important files, thinking before you click, configuring browsers to protect you, staying current on what is going on in the world of viruses so you will know when you might have one and what to do.

This issue of IRM News covers most of these topics. But we encourage you to go online and read more. A good place to start is the National Cyber Security

Alliance's web site Stay-SafeOnline.org (<http://www.staysafeonline.info>)

Quick Tips for Being Safe Online

- Defend your computer with firewalls, antivirus and antispyware applications, and keep up with security updates. Systems supported by IRM already have firewall activated.
- Use strong passwords, keep them secret, and change them regularly. For information on creating a strong password, see the article in this issue.
- Think first. Click later. Or be suspicious of everyone. Before you open an attachment, be it from e-mail or even an instant message, think about it. If you don't know who sent it to you, just delete it. Even if you know the sender, consider if you really want, or need, to open it. Remember that hackers will do all sorts of things to get you to open the attachment - they need your cooperation. Subject lines will likely be something innocuous or

appealing. Beware especially of ones that claim to be at "your request." If you haven't made any requests, delete the message. And don't follow links that say they'll clean your machine of viruses - most likely the site will give you a virus.

- Think for a long time before you give out your personal information. Never give your sensitive information in an e-mail and don't even consider giving it in a pop-up window (too much of a chance that spyware will get it).
- Know what is done with your personal information when you give it on a website. Read the privacy statements carefully. Make sure the site is secure (has https in the URL and/or you see the padlock or an unbroken key in the lower corner of the browser window). A secure site means that what you enter and send via the webpage is encrypted, thus harder to steal and use.
- Do not keep files with sensitive information (such as Social Security or credit card numbers).

FIREWALLS—THE GUARDIAN AT THE GATE

Large buildings, such as apartment complexes, have firewalls in them - a solid, windowless/doorless fireproof wall that prevents fire from spreading from one part of the building to another. Computers and networks also have firewalls (in some instances called Border Protection Devices) that keep hackers and potentially harmful programs from getting in. The firewall's job is to keep people out of your computer or net-

work. It is because of the firewall that if you bring a laptop computer on campus and want to connect it to the network that you must first log onto the network (aka **authenticating**). It's also because of the firewall that you can't automatically use Remote Desktop from home to connect to your campus computer.

The Windows XP and Macintosh OS X operating systems also

have a built-in firewall that gives your desktop computer some added protection in addition to the university firewall. Follow this link for a video on using the Windows XP firewall: <http://security.getnetwise.org/tools/firewallxp-instruct>. For information on the Macintosh firewall, go to <http://security.getnetwise.org/tools/firewall-osx-instruct>.

COMPUTER VIRUSES: WHAT THEY ARE AND HOW TO PROTECT YOURSELF

Computer viruses are programs that, like biological viruses, can replicate themselves, spread from one computer (or body) to another, and generally cause problems. Today there are various types of programs that spread among computers, and they are collectively called “malware” (**malicious software**). Depending on the form of malware, the damage can be just annoying (lots of pop-up ads, or otherwise slowing the performance of your computer) to downright disastrous (causing you to reformat a harddrive). If your computer starts acting “strangely,” then you might have a low level virus.

Regardless of the level of damage, it’s worth protecting your computer from them. Not doing so can harm your computer and unknowingly spread it to other people. You don’t even have to sneeze or shake hands

to spread a computer virus!

But How Do I Get the Viruses?

These days most viruses travel through the Internet, primarily by e-mail. The best rule of thumb is not to accept attachments that you are not expecting or don’t know about. So many jokes travel via e-mail, and many of them by attachment. Why risk it? At FAU, we have virus scanners on the e-mail servers which analyze attachments for viruses. If an attachment is found to contain a virus, the attachment is removed from the e-mail message; you still get the e-mail but there will be a notice that an attachment was removed.

And How Can I Protect Myself?

The best way to protect your computer is with antivirus software. To continue the biological analogy, antivirus software works similarly to a flu shot – it recognizes the virus and keeps

it from infecting your machine. And just as flu vaccines have to be reformulated every year because the flu virus mutates, so the antivirus software has to be updated routinely because the computer viruses are constantly being changed or reinvented. The antivirus software stores virus definitions (ways to recognize the viruses), so you routinely need to update your antivirus definitions.

IRM provides Symantec AntiVirus to all FAU faculty and staff to protect individual computers, hence the entire campus, from viruses. Once you’ve installed the AntiVirus client on your computer, it routinely checks an FAU server for updated virus definitions. The software does this automatically so you don’t need to worry about keeping up with it (unlike having to remember to get a new flu shot every year). However, you can also update the virus definitions manually, in

case your computer has been off for some length of time (your computer needs to be on and connected to the network for the automatic updating to work).

New virus definitions are usually released by Symantec weekly. However, if high-vulnerability threats occur, new virus definitions are released more frequently. All updated definitions are automatically installed on your computer by the FAU virus definition update server.

If you have any questions about antivirus software, contact your college computing consultant or the IRM help desk.



POP-UPS AND POP-UP BLOCKERS

Pop-up windows are the windows that open when you click on something on the web, and sometimes they seem just to open themselves. They have become a standard practice on the web, and some web applications use them legitimately. For example, MyFAU’s e-mail and calendar clients open via pop-up windows. But pop-ups can also be a result of spyware or adware, and, perhaps most dangerously, can also be used by malware for gathering personal information. A good rule of thumb is never enter your personal information in a pop-up window.

The good news is that you can block pop-ups, but blocking all pop-ups can be dangerous because some web applications use pop-ups to provide information or functionality.

Microsoft Internet Explorer, Mozilla Firefox, Safari, and AOL browsers have pop-up blocker options in their tools/preferences. (See information below on setting the pop-up blocker in these applications.) Microsoft has also included a pop-up blocking feature in the Windows XP operating system – it was released in Service Pack 2.

Blocking pop-ups can greatly reduce the annoyance and damage from spyware, but you need to be aware that it can also decrease the functionality of some programs. Turn the pop-ups off as needed. With most pop-up blockers, you can temporarily override the blocking by holding the control key when you click or you can identify sites whose pop-up you will accept (for example, accept pop-ups from MyFAU and

Blackboard).

Also keep in mind that if a program isn’t working as you would expect (especially if nothing happens when you click on an icon that should open a window) then you should review your pop-up settings.

Internet Explorer Pop-up Blocker

1. From the Tools menu select Internet Options.
2. Select the Privacy tab. Near the bottom of the window is a section labeled Pop-up blocker.
3. If the checkbox for “Block pop-ups” is blank, the pop-up blocker is not on. To turn on the pop-up blocker click the box so that it is checked.
4. Click the Settings button so you can customize what is

actually blocked.

Mozilla Firefox Explorer Pop-up Blocker

1. From the Tools menu select Options to open the options window.
2. Click the Web Features button.
3. If the checkbox for “Block Popup Windows” is blank, the pop-up blocker is not on. To turn on the pop-up blocker click the box so that it is checked.
4. Click the Allowed Sites button to enter the URLs for sites whose popups you want to accept (for example, enter <http://myfau.fau.edu> to accept pop-up windows from MyFAU.

ALL ABOUT SPAM AND DEALING WITH IT

Spam is the electronic form of junk mail consisting of commercial advertising, often for questionable products, get-rich-quick schemes or quasi-legal services. At the minimum, spam is an annoyance because e-mail users have to spend time to sort through and delete the messages. But to appreciate the magnitude of the problem of spam, think of how many messages a day you get, and then multiply that by the number of FAU e-mail users (approximately 30,000). It is estimated that 50-75% of all e-mail coming into the university mail servers is spam. Every one of those messages is taking up space on the mail servers, and it takes time to deliver each message as well. But the real damage of spam goes beyond its consumption of resources; some spammers are now using the method for identity theft.

Spam and Identity Theft

It can't be said too often: Never give your personal information via an e-mail. No legitimate business, especially a financial institution, is going to send you an e-mail and ask for your account number, username, and password. And that is exactly what the malicious spammers (called phishers) do. If for some reason an institution wants you to verify your information (which is the line most phishers or identity thieves use to get you to send your information), it will instruct you to log into the secure site and verify the information there. When in doubt of the legitimacy of a message, forward the message to the institution that supposedly sent it and ask if it's legitimate.

How to Avoid Spam Altogether

Spam has been a hot topic for some time now, and people in the university are always asking IRM to "do something" about it. Keeping spam out is very difficult, however, because unlike with viruses, there is no foolproof way to detect spam. The university community has made it clear that it can't risk losing legitimate e-mail, so FAU has implemented anti-spam software on two levels. The first level is to deal with messages that come from known spam sites. Unfortunately, those sites change frequently and the list of known sites is very small. Second is to scan messages that have characteristics of spam. For example, since we know that spammers send their message to a large list of people, the anti-spam software looks for messages sent to a list of 25 or more addresses. Also, since much spam is for certain products or activities (Viagra and physical enhancement, for example), the software looks for keywords to identify spam. Such messages will be delivered to your inbox with "SPAM:" added to the beginning of its subject line.

Messages sent from a known spam site are returned to the sender and not delivered to the intended recipient. If you send to a distribution list or many FAU e-mail addresses, it is possible your message

would be stopped as spam. You can request that the list be put on the "White List" so that it will be delivered without the "SPAM" designation. Send your request to the IRM Help Desk (3999@fau.edu). The request to put a site on the "White List" is subject to management approval.

Dealing with the Spam in Your Mailbox

The method described above isn't perfect because it means we all still get a lot of spam in our mailboxes, but at least it makes it easy for us to find it. You can then set up rules or filters in your e-mail client, so that all mail designated as spam gets put into a separate folder. That way your legitimate and important mail messages aren't lost in a sea of spam, and you can easily scan through the spam and delete as needed.

Filtering Spam in Outlook

To create a Rule in Outlook 2003 to filter messages with **SPAM:** in the subject follow these steps:

- Start Outlook.
- Open your **Inbox** folder.
- From the Menu bar, click **Tools-> Rules and Alerts...**
- Click the **New Rule** button. The Rules Wizard window will open.
- Select **Start creating a rule from a template** and then, in Step 1 of the window, select **Move messages with specific words in the subject to a folder**.
- Under **Step 2: Edit the rule description**, click on the link

"**with specific words in the subject.**"

- In the field **Specify words or phrases to search for in the subject**, enter **SPAM:** (Note: Be sure to include the colon after the word **SPAM:** as shown)
- Click **Add. "SPAM:"** will then appear in the **Search List**.
- Click **OK**.
- Then click on the link "**move it to the specified folder**" (also located under **Step 2: Edit the rule description**).
- Select the **Junk E-mail** folder (Alternately, you can have spam sent to a folder called **SPAM**, to another folder you specify, or to a new folder by clicking the **NEW** button to create a new folder).
- Click **OK**.
- Click the **Finish** button.
- A rule called **SPAM:** will appear at the top of the **Rules and Alerts** window.
- Click **OK** to save changes.

Once you have this rule established, all incoming mail with **SPAM:** in the message subject will be sorted into your **Junk E-mail** folder (or the folder name you specified).

Periodically review your **Junk E-mail** folder, since at times legitimate messages do end up in the **Junk E-mail** folder, because of the Microsoft Outlook internal configuration, and it is beyond the user control.

For information on filtering spam in MyFAU or Outlook go to <http://www.ecs.fau.edu/training/coursematerials.htm>

WHY YOUR AOL ACCOUNT ISN'T RECEIVING FAU E-MAIL

Just as FAU attempts to protect FAU e-mail users from spam, so do the major ISPs (Internet Service Providers), such as AOL, Yahoo!, and Hotmail. Many people in the FAU community have noticed that they are not getting FAU mail delivered to their AOL account, or if it is delivered it is delayed. This situation occurs because AOL, like FAU, considers messages likely to be spam if they are sent from a single address to many AOL users.

FAU has discussed the problem at length with AOL administrators, but AOL has not been willing to change its procedures. Other universities are facing the same problem and have strongly recommended that their faculty, staff, and students not forward their e-mail because of the potential for the mail to be blocked. IRM also recommends that you not forward your FAU e-mail to such accounts. FAU is now using e-mail for much of its communi-

cation – student bills, financial aid disbursements, emergency notices. FAU can control mail only while it's on our campus or servers. So if your mail is forwarded to a non-FAU account and doesn't arrive, IRM's ability to troubleshoot is extremely limited.

To ensure that you receive your FAU e-mail, IRM recommends that you not forward it to an AOL, Hotmail, or Yahoo! account.



PASSWORDS—SECURITY STARTS WITH YOU

Computer security comes in many forms, but it always starts with individual user logins and good, strong passwords. Some time ago the conventional wisdom was that a password should not be anything that someone could associate with you, such as any form of your name, pets' names, family member's names, etc. While that is still good advice, that's only the beginning. You need to protect your password, and what it protects for you, from people who don't know you. People who want to break into computers can run programs that attempt to "crack" individual passwords by trying words from a dictionary. The more mundane your password is, the faster the person can crack it.

Therefore, IRM recommends that your password never be a word that can be found in the dictionary. Passwords should also always involve a combination of letters,

numbers, and symbols.

FAU is committed to securing its IT environment, but you need to do your part by having a strong password, changing it routinely, and keeping it secure (that means not taping it to the bottom of your desk or keyboard). Read below for more information on good passwords and keeping your computing secure.

FAU requirements for passwords

- must be 5-20 characters in length
- must contain a mix of letters and digits (at least 1 of each)

Recommendations for a secure password

- Use a combination of capital and lower case letters, numbers and symbols (eg., ! @ # \$ % ^ & + -)
- Never use your username as your password

- Never use any form of your name, pet's name or other name associated with you
- Never use a word found in the dictionary
- Change your password regularly, at least every 90 days



Examples of good passwords

Password	What makes it secure
%Om&Ber	Variation of "bomber" that uses combination of punctuation and numbers for letters
T*x4\$M8n	More than 6 characters; numbers, punctuation, and mix of upper and lower case letters
j@T&PI4Ne	Two words, separated by punctuation, using upper and lower case letters, and numeric substitution

SPYWARE

Like viruses and other malware, spyware is at best annoying, and at worst malicious. It is software that you unknowingly install when you download and install other software. For example, if you install some kind of weather or news feed to your computer, it's possible that the application has inside it some kind of spyware that isn't mentioned in the license and use agreement. Spyware can cause serious problems, compromising your computer's security and potentially sending sensitive information, such as passwords or credit card numbers, to the spyware's creator.

One of the most common forms of spyware is adware,

advertising software, that will either run in the program window itself or in pop-up windows. These advertisements are usually for legitimate products, but they can still be annoying if not intrusive. They can track the web sites you visit and then send that info back to the advertiser. Some people might defend the practice as market research, but the activity can interfere with your computer's performance, especially if it gets to the point that you have so many pop-up windows opening that you can't effectively use your computer.

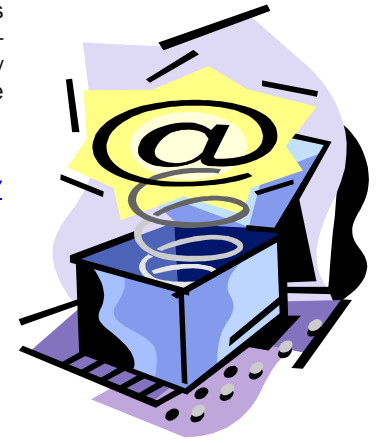
The good news is that there are several software applications that detect and remove

spyware and other malicious programs from your computer. You can safely download these from the Internet at no charge:

Ad-Aware:
<http://www.lavasoftusa.com/>

Spybot:
<http://www.safer-networking.org/en/download/>

Microsoft Anti-Spyware:
<http://www.microsoft.com>



The Most Common Signs that Spyware is on Your Computer

- Bombarded with pop-up ads, especially if you get pop-up ads when you're not browsing the Web, or when you first turn your computer on.
- Web browser settings have changed, and you didn't change them or you can't change them back. For example, when you open your web browser it uses something other than what you had set as its home page.
- Web browser now has new components or options in its menus or toolbars. If you have spyware it's also likely that even if you remove the toolbars they'll reappear the next time you start your web browser or restart your computer.
- Computer seems to be running slowly, and gets slower all the time. Spyware does its work without you seeing it, but it's using your computer's memory and processing resources, so it can slow down your machine. In addition to the machine running more slowly, you might notice some programs "crashing" (just quit working) often, or more often than normal.

Types of Malware

Viruses – often embedded in e-mail messages as attachments. When you open the attachment, the virus program is activated and goes to work. Consequently, do not open attachments you are not expecting or that are from someone you don't know very well and know why they are sending you the attachment.

Worms – similar to viruses but don't need a host file to spread. Worms typically use a vulnerability in a computing system or some other method to trick users into starting them.

Trojan (Trojan Horse) – as the name suggests, it's something that appears harmless, even good, but contains something malicious and dangerous. Unlike viruses and worms, they don't replicate. They can be attached to legitimate software, or spyware, so you don't know it's there. A common result of Trojans is a lot of adware/spyware that causes many popups and ultimately making it near impossible to use a web browser.

Spyware – software that watches how you use your computer and sends the information to whoever is collecting it. Adware, which watches what sites you go to and what you do on them is a kind of spyware. Although spyware doesn't necessarily corrupt your computer, its activity can hurt your computer's performance (for example, windows might open more slowly than usual).

Exploit – software that takes advantage of known security vulnerability. One way to protect yourself from exploits is to keep current with patches for your operating system (Microsoft sends out new service packs when security vulnerabilities or exploits are found).

Key Logger – records all key strokes to a file which is then sent to the hacker. Key loggers are dangerous because they can record login and password or other sensitive information (such as credit card numbers). With that information, a hacker can do a lot of damage.

**FLORIDA ATLANTIC
UNIVERSITY**

Jeffrey Schilit, CIO

schiliti@fau.edu

Information Resource Management

777 Glades Road

Boca Raton, FL 33431

IRM Help Desk

Phone: 561-297-3999

E-mail: 3999@fau.edu