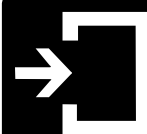




Inside OIRT



The Office of Information Resources and Technology Newsletter
Fairleigh Dickinson University

Volume 3, Issue 2

January 2006

Inside OIRT -

Third Issue

Welcome to Spring '06 and the third issue of **Inside OIRT** - the newsletter from The Office of Information Resources and Technology (OIRT). OIRT consists of University Systems and Security, Computing Services, Telephone and Voice Services, and Management Information Systems. For more information on these organizations and the services and support each provides, please visit the <http://isweb.fdu.edu> website.

The newsletter will be published twice yearly, at the start of the Fall and Spring semesters, and will provide the FDU community with useful information related to technology, new services or capabilities, developing trends, how to's, and tips and tricks.

Archival copies of **Inside OIRT** will be available on the <http://isweb.fdu.edu> website. ■

Managing Malware

Dealing with insidious programs

There are a lot of computer programmers out there that write software applications to steal information, wreak havoc on computer systems and user data, or to attack computer systems and networks to interrupt important services. This computer code, collectively referred to as malware, is often developed for competitive advantage, financial gain, or to facilitate illicit or illegal activities. Some malware is developed simply for the fun and challenge of it. That is, it was developed because it could be, often to exploit a security flaw.

High speed internet-working provides the mechanism to deliver these insidious applications to your desktop at alarming rates. End users must be aware of the various forms of malware, and the various delivery strategies, in order to safeguard their valuable information.

This issue of **Inside OIRT** focuses on the various types of malware that is presented to our community on a daily basis. It includes email viruses, spam, phishing, and spoofing. Although FDU employs techniques to minimize invasion and provides its' end user community with tools to help thwart malware, the best defense against falling victim to a malware attack is to be well informed, to be suspicious of all email and websites, to remain on guard, and to take proactive measures.

There is no technological solution that will completely halt malware. However, a proper set of tools and an educated user base will help to mitigate the risks of a malware attack, and will help to make the personal computing experience at FDU safer and more enjoyable. ■

INSIDE THIS ISSUE

THEME: MANAGING MALWARE

1	Inside OIRT – Third Issue
2	Managing Phishing
2	New Webmail System Coming
3	Wireless Hot Spots
4	Managing Spoofing
4	The UTAC
5	Managing Spam
6	Managing email Viruses

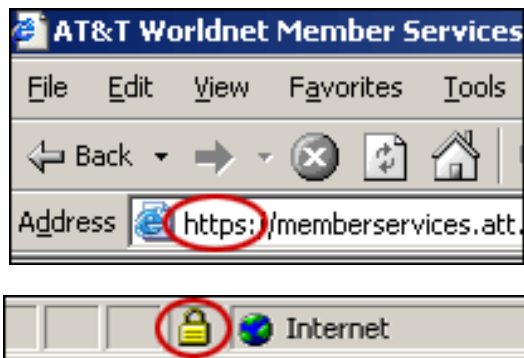
Managing Phishing

I've heard about a scam called "phishing." What is it?

It's a kind of identity theft whereby spammers "fish" for consumers they can trick into giving them personal information. They accomplish this by sending you what looks like a legitimate e-mail message from a reputable company. The e-mail may ask you to update your credit card information, billing information or social security number. If you respond to this type of e-mail, spammers can get your personal information and then use it for their own purposes and without your permission.

Be suspicious!

- FDU, and most legitimate companies, will never ask customers to provide credit card information or a social security number in e-mail.



- If the e-mail links you to a website that appears to be a company website and asks for personal information like a password or credit-card or Social Security number, look for the "lock" icon on the browser's status bar or an "s" after the http in the address. Both indicate that your information will be secure during transmission. (For an exception, see below.) If these symbols aren't present, DO NOT enter your personal information!

- Recently, some phishing scammers have been able to create the image of a "lock" icon on their fake websites. If you receive an e-mail requesting confidential information that links you to a website and you see the padlock in the browser's status bar, you should still be suspicious. Take the safe approach and call the company to give the information over the phone.
- No phone number listed on the site? Still not sure the request is legitimate? Close the e-mail or its website and locate the business's website using a search engine. Contact the company based on the information you get from the search to confirm the request is legitimate.



New Webmail is coming!

New Webmail system to be deployed in '06

A new email system is planned for deployment in early 2006. The new email system will have an improved web interface (Webmail.fdu.edu) and vastly improved speed, performance, and availability. Additionally, the new email system will have features that our university community has been requesting such as calendaring and spam filtering.

For those that prefer to use a mail client instead of the web interface, the new email system will continue to work with all common clients such as Internet Explorer, Netscape, Thunderbird, and Pegasus Mail, and there will be greater integration with Microsoft Outlook.

The deployment of a new email system is a complex task. However, it is our plan to deploy the new email system with little or no disruption to Webmail users. As we progress with the deployment plan over the next several weeks you can expect more details on the rollout such as the date of initial deployment, information about new features and capabilities, and sources for help.



Wireless Hot Spots

Where to get connected

Metropolitan Campus

- Alumni Hall - General coverage throughout the entire building.
- Bancroft Hall - General coverage throughout the entire building.
- Becton Hall - General coverage throughout the entire building.
- Dickinson Hall - General coverage throughout the entire building.
- Edward Williams Building - Available in the administration office.
- Fitness Center - General coverage throughout the entire building.
- Muscarelle Center - General coverage throughout the entire building.
- Rothman Center - General coverage throughout the entire building.
- Student Union Building - General coverage throughout the entire building.
- University Hall - Available in the administration office.
- Weiner Library - General coverage throughout the entire building.

College at Florham

- Campus Library - General coverage throughout the entire building.
- Dreyfuss Building - General coverage throughout the entire building.
- East Cottage - General coverage throughout the entire building.
- Ferguson Recreation Center - General coverage throughout the entire building.
- Mansion - General coverage throughout the entire building.
- Rothman Institute - General coverage throughout the entire building.
- Science Building - General coverage throughout the entire building.
- Stadler, Zenner Academic Building - General coverage throughout the entire building.

- Student Center - General coverage throughout the entire building.
- Twombly Residence Hall - Available in the lounge area.
- West Cottage - General coverage throughout the entire building.

Nearly 250K PCs Turned Into 'Zombies' Daily

By Gene J. Koprowski, TechNewsWorld 1/06

December was a record month of new zombie activity reaching 7,609,465 total infected IPs. The largest number of infected IPs continues to alternate between the U.S. and China, primarily due to the large number of computers coming online for the first time.

The term "zombie" is used to describe a personal computer being used to perform a task or tasks without the owner's knowledge. These tasks may include sending [spam](#), serving pornography, or performing denial of service attacks.

CipherTrust said that since the Sober outbreak in November, the number of new zombies sending spam and virus messages increased by nearly 50 percent, bringing the average total number to more than 250,000 new infected Internet Protocol (IP) addresses each day.

This increase made December a record month of new zombie activity reaching 7,609,465 total infected IPs. The largest number of infected IPs continues to alternate between the U.S. and China, primarily due to the large number of computers coming online for the first time.

According to the research, the average number of daily new zombies for December was 247,755, and the total number of new zombies for December: 7,609,465.

Beware of the zombies! ■

Managing Spoofing

What is spoofing?

Spammers use e-mail spoofing to trick you into believing the e-mail you're receiving from them came from someone else, usually a trusted source. For example, it could appear to be from the system administrator at FDU, or that of your Internet Service Provider or a local authority. The e-mail requests that you provide personal, private or financial information.

Remember the rule!

- Never send personal, private or financial information in e-mail. Pick up the phone and call whoever is asking for it or find the company's secure website where you can look for the "lock" icon on the browser's status bar or an "s" after the http in the address. Both indicate that your information will be secure during transmission.

Why do I receive spam that is not addressed to me?

There are a few reasons that you may receive e-mail that is not directly addressed to you in the To: field. First, your e-mail address may actually be listed in the BCC: field (Blind Carbon Copy). A second possibility is that the address listed in the To: field is actually the name of a list that includes your e-mail address. There are many scripts on the Internet that build lists of e-mail addresses. There are several ways in which your e-mail address can become part of a list:

1. If you have ever asked to be unsubscribed from a particular e-mail group, you have unknowingly sent your e-mail address to the list creator.
2. When you are viewing a web site, the creator of this site may have a script asking you to accept a "cookie.". By accepting this cookie, the author of the web site is given certain information about you. This information includes your e-mail address, signature, browser and IP address. It is best to

direct your browser to warn you before accepting cookies.

3. It is also possible that you have joined an e-mail list by:
 - a. Software Registration
 - b. Filling out an on-line form
 - c. Responding to a survey ■

The UTAC

University Technical Assistance Center

The Fairleigh Dickinson University Technical Assistance Center (UTAC) is the university technical helpdesk support organization. Fairleigh Dickinson University students, faculty, and staff must contact the UTAC to initiate support requests for commercial application software, desktop environments and peripherals, network connectivity, computer password maintenance (i.e., Novell, Webmail, Unix, Datatel), hardware and software configuration support, other computer related product and service issues, Blackboard, and cable TV repair requests. The university community also has access to knowledgebase information for self-service exploration of remedies, or to seek answers to frequently asked questions.

For students, the University ID is your student identification number. For staff and faculty, the University ID is your employee number. It is important for you to remember, and keep for reference, your University ID number now, and in the future, as more and more services will be offered using the University ID number as the key to unlock these services.

The FDU Technical Assistance Center (UTAC) can be reached via phone at 973-443- 8822, from The College at Florham by dialing the digits 8822, from The Metropolitan Campus by dialing #8822, via email at FDUTAC@fdu.edu, or the self service web portal from the <http://inside.fdu.edu> website. ■

Managing Spam

How do spammers get my e-mail address?

Spammers harvest e-mail addresses in various ways including scanning chat rooms, searching the Web, and buying online mailing lists (often from other spammers).

Protect Yourself:

Be cautious when giving out your e-mail ID. Read the privacy policies of Websites where you list your e-mail ID to understand each site's policy for distributing or selling e-mail IDs. FDU never sells or gives away e-mail addresses to anyone.

Why do I keep getting messages promoting the same products over and over again? Can't Spam Blocker filter these messages out?

Spammers constantly change their apparent addresses (the ones you can see in the "From:" field) and their actual addresses (the numerical addresses that identify their mail systems). If you get a junk e-mail and then get the same one again, chances are the spammer is launching several attacks under different addresses.

Note that most spam blockers works reactively. That is, once a spammer has launched an attack, spam blockers identify it and blocks further messages in that attack from hitting e-mail inboxes. This is a highly effective strategy as it sidelines over 70% of incoming mail as spam and reduces the chance of blocking important messages you want to receive.

While it may seem effective to block certain words occurring in spam messages, spam blockers do not do that because it would amount to censoring the mail system. Also, spammers think of ways to alter spellings that, while still readable by humans, could never be foreseen and coded into filters.

Finally, though it may not provide much consolation, it's important to note that the mail experience among all FDU users varies widely, with many people seeing very little spam in their inboxes. If you are seeing large volumes of spam in your inbox, review our tips

on protecting your address, below.

What can I do to protect my e-mail address?

1. Create several addresses that you can use for different purposes. For example, safeguard your WebMail address for academic or university business only. Then, create other addresses using Yahoo, hotmail, etc., to give out when registering for services on the Net or for commercial Web sites and newsletters (i.e., sites that are likely to be farmed by spammers for e-mail addresses), and another to give out to friends for personal messages.
2. Create a separate e-mail address if you participate in any message boards or USENET newsgroups. Automated programs that collect addresses scan these forums constantly. If you post to boards and newsgroups, you are almost certain to get spam. Protect that address with the tools mentioned above in #1.
3. Avoid putting your address on any Web page, especially in a "mailto:" link. Again, spammers search out these addresses and add them to their mailing lists.
4. If you want your address to be available on a Web page, consider altering it so that it can be interpreted by people but not by machines, a process called "munging." Here are some easy ways to munge your address:

--username@NOSPAMatt.net
--usernameATattDOTnet
--username@att.REMOVETHIS.net
5. Avoid opening messages that look spammy. Often, a spam message will contain a bit of code that allows a spammer to know if it has been opened by the recipient. Opening a message like this will simply confirm to the spammer that your address is valid, ensuring that it will stay on his list and will likely be distributed to other spam lists.

continued on page 6

Managing e-mail Viruses

What is an e-mail virus?

An e-mail virus is a small program usually sent as an attachment to an e-mail message. It is created specifically to invade computers and wreak havoc on them. If activated, the virus will carry out an unwanted procedure on your computer, potentially damaging all of the user data and system files.

One common e-mail virus is a self-propagating "worm" that, when you open the e-mail attachment, automatically sends itself to random addresses in an e-mail address book. Some worms are harmless. Some can destroy files on the computer's hard drive.

What is FDU doing to fight e-mail viruses?

We are always trying to make your e-mail safe. We have enabled anti-virus technology on your Webmail e-mail account to protect it, and we offer free anti-virus software to students, and to staff and faculty for their university desktop or laptop. The use of our enterprise edition of Norton Anti-Virus protects users without the need of maintaining costly anti-virus definition annual subscriptions.

Because you can get viruses in ways other than opening infected e-mail attachments, it's mandatory to maintain a virus protection program on your computer and use it daily. The university has standardized on the enterprise edition of Norton Anti-Virus and provides it to students, faculty, and staff and no cost. It will help protect your computer from viruses that may be present in files you download from the Internet or on disks you share with friends.



"Yesterday is history. Tomorrow is a mystery. And today? Today is a gift. That's why we call it the present." Babatunde Olatunji

For comments and suggestions about this newsletter, please contact Jim Lebo at jlebo@fdu.edu

Why am I receiving bounce back messages for spam that I did not send? What can be done to prevent this?

Junk mailers often will randomly select an e-mail address from their list and insert it as a forgery into the 'From' or 'Reply To' line in an effort to avoid detection. In some cases, hundreds of bounce back messages and removal requests then go to the unfortunate owner of the forged e-mail address.

The majority of mail clients have filtering features that will enable you to filter out and auto delete any unwanted bounce back messages and/or removal requests.

Unfortunately, nothing can prevent a spammer from forging your address if they already have it. Please see the FAQ on protecting your e-mail address for recommendations on safeguarding your address from spammers.



Did you know?

- Especially during winter storms, weather safety may require closing of FDU campuses for a day or portion of a day. The best way to stay abreast of the latest news is to call FDU's voice mail, which will provide a message regarding the University's status (open, delayed opening, closed, etc.). The switchboard also will have up-to-date information on related matters. A third way to get information is to log onto the University Web site (www.fdu.edu) where a banner will indicate any delayed opening or closing information.
 - The FDU academic computer labs will open or close as student safety permits.
- Completing a UTAC customer satisfaction survey automatically enters you into a drawing for \$50 of Fairleigh 1Card Cash. Visit <http://fairleigh1card.com> for more information on the Fairleigh 1Card program.

