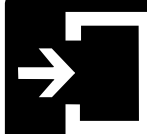




# Inside OIRT



The Office of Information Resources and Technology Newsletter  
Fairleigh Dickinson University

Volume 1, Issue 1

January 2005

## Inside OIRT -

### *Inaugural Issue*

Welcome to the inaugural 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 [isweb.fdu.edu](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 [isweb.fdu.edu](http://isweb.fdu.edu) website. ■

## Password Maintenance

### *Do's and Don't*

The objective when choosing a password is to make it as difficult as possible for a hacker to make educated guesses about what you've chosen. This leaves the hacker no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even when conducted on a machine that could try one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete.

### What Not to Use

- Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
- Don't use your first or last name in any form.
- Don't use your spouse's or child's name.
- Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- Don't use a password of all digits, or all of the same letter. This significantly decreases the search time for a hacker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use a password shorter than six characters.

### What to Use

- Do use a password with mixed-case alphabetic characters.

## INSIDE THIS ISSUE

THEME: PROTECTING INTELLECTUAL PROPERTY

1	Inside OIRT – Inaugural Issue
1	Password Maintenance – Do's and Don'ts
2	Care of LCD Screens
2	Safeguarding Data – Gone Phishing
4	The UTAC
5	Backing Up
5	Apply Patches and Anti-Virus
6	Did you know?

*continued on page 4*

## Care of LCD Screens

### *Do's and Don't*

One of the most expensive components of a computer system or laptop is the LCD monitor or screen. Liquid Crystal Display (LCD) screens are easily susceptible to damage and scratches, so it's a good idea to make sure that you don't touch the display surface and that you clean the screen correctly.

*Not all types of cleaning solutions are acceptable for LCD screens.* Using ethyl alcohol or ammonia - based cleaners repeatedly may cause permanent damage to the LCD. Over time, using these types of cleaners could cause the surface of the screen to yellow. It can also make the screen brittle and eventually cause cracking on the screen surface.

The following cleaners should **NOT** be used:

- Acetone
- Ethyl alcohol
- Ethyl acid
- Ammonia
- Methyl chloride

The following types of cleaners are acceptable:

- Water
- Vinegar (mixed with water)
- Isopropyl Alcohol

Some basic supplies needed to clean an LCD screen include:

- A soft cotton cloth. When cleaning the LCD screen it is important to use a soft cotton cloth, rather than an old rag. Some materials, such as paper towels, could cause scratches and damage the LCD screen.
- A solution of water and isopropyl alcohol. This solution can be used along with the soft cotton cloth.
- Computer wipes. Use these only if they specifically state on the package that they are designed for LCD laptop screens. Computer wipes can come in handy for fast clean-ups or when you want to avoid mixing up a cleaning solution yourself.

To clean the LCD surface properly:

- Do not spray any liquids on the LCD screen

*continued on page 3*

## Protecting Your Intellectual Property

### *Gone Phishing*

Email schemes, called "phishing" or "carding", are an attempt to trick consumers into disclosing personal and/or financial information. The emails appear to come from companies with whom consumers may regularly conduct business (e.g., AOL, Earthlink, Paypal, eBay, or a credit card issuer). Often times the email threatens termination of accounts unless consumers update billing information. Caution should always be used when receiving any unsolicited communication requesting personal information.

Many of these email schemes contain links to "look-alike" websites that are loaded with actual trademarked images. The websites then instruct consumers to login to their accounts and/or "reenter" their credit card numbers, social security numbers, bank PINs, or other personal information. If consumers actually provide the information requested, the data goes to scammers, not the legitimate company whose name is on the site. Thereafter, the data is often used to order goods or services and/or to obtain credit in the name of the consumer.

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them. A lot of people are being fooled.

The FTC, the nation's consumer protection agency, suggests these tips to help you avoid getting hooked by a phishing scam:

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate

*continued on page 3*

companies don't ask for this information via email.

- If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.
- Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Use anti-virus software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.
- A firewall helps make you invisible on the Internet and blocks communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, "patch" your system to close holes in the system that hackers or phishers could exploit.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.

Suspicious e-mail can be forwarded to [uce@ftc.gov](mailto:uce@ftc.gov), and complaints should be filed with the state attorney general's office or through the FTC at [www.ftc.gov](http://www.ftc.gov). ■

directly, and do not use paper towels, as this can cause the LCD screen to become scratched.

- Always apply the solution to your cloth first, not directly to the parts you are cleaning. You want to avoid dripping the solution directly into the electronics of your display, computer, or laptop.
- Stroke the cloth across the display in one direction, moving from the top of the display to the bottom.

Occasionally clean your computer as follows:

- Use a soft cloth moistened with non-alkaline detergent to wipe the exterior of the computer.
- Avoid spraying cleaner directly on the display or the keyboard.
- Gently wipe the display with a dry, soft cloth.
- Laptop users: If you see a scratch like mark on your display, it might be a stain transferred from the keyboard, or the TrackPoint (R) pointer, when the cover was pressed from the outside. Wipe or dust the stain gently with a soft, dry cloth. If the stain remains, moisten a soft, lint-free cloth with water that does not contain impurities, wring out as much of the water as you can, and then gently wipe the display again. Be sure to dry the display before closing the laptop.

**Prior to the use of any cleaning agent, be sure to read and understand the manufacturer label regarding hazards, handling, and proper usage.**

Avoiding unnecessary LCD screen contact and proper cleaning of the LCD screen will be rewarded with years of service, best picture quality, and insurance against costly damage. ■



## 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.UTAC, from The College at Florham by dialing the digits 8822, from The Metropolitan Campus by dialing #8822, via email at [FDUTAC@fdu.edu](mailto:FDUTAC@fdu.edu), or the self service web portal from the <http://inside.fdu.edu/> website. ■



- Do use a password with nonalphanumeric characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

### **Method to Choose Secure and Easy to Remember Passwords**

- Choose a line or two from a song or poem, and use the first letter of each word. For example, "In Xanadu did Kubla Kahn a stately pleasure dome decree" becomes "IXdKKaspdd."
- Alternate between one consonant and one or two vowels, up to eight characters. This provides nonsense words that are usually pronounceable, and thus easily remembered. Examples include "routboo," "quadpop," and so on.
- Choose two short words and concatenate them together with a punctuation character between them. For example: "dog;rain," "book+mug," "kid?goat."

Most of all, **SAFEGUARD AND REMEMBER YOUR PASSWORDS**. Password reset requests are the most common support request type to the UTAC. Such requests drive up call holding times and support costs.



## My Laptop Freezes Up!

### *Intermittent Memory Problem to Blame*

Some of the newly issued IBM faculty laptops are experiencing a 'hanging' or 'freezing' problem. This problem has been attributed to intermittent memory problems.

If your university issued IBM ThinkPad is exhibiting this behavior, please contact the UTAC, at x8822, to arrange having the laptop memory replaced. ■

## Protecting Your Intellectual Property

### *Backing Up*

There are many ways you can unintentionally lose information on a computer. A child playing the keyboard like a piano, a power surge, lightning, floods, accidental erasure, and sometimes equipment just fails. If you regularly make backup copies of your files and keep them in a safe and separate place, you can get some, if not all, of your information back in the event something happens to the originals on your computer.

Deciding what to back up is highly personal. Anything you cannot replace easily should be at the top of your list. Before you get started, make a checklist of files to back up. This will help you determine what to back up, and also gives you a reference list in the event you need to retrieve a backed-up file. Here are some file suggestions to get you started:

- Bank records and other financial information
- Digital photographs
- Software you purchased and downloaded from the Internet
- Music you purchased and downloaded from the Internet
- Personal and professional projects and important correspondence
- Your e-mail address book
- Your Microsoft Outlook calendar
- Your Internet Explorer bookmarks

There are many media options in which to backup your data. All members of the FDU university community are granted network storage and the university IBM personal computers are equipped with CD-RW drives that allow for backup onto CD. USB "thumbdrives" have become a convenient and economical way to back up important data.

For more information on backing up to the network drive, or to CD-RW, please visit [isweb.fdu.edu](http://isweb.fdu.edu). ■

## Protecting Your Intellectual Property

### *Apply Critical Updates & Anti-Virus*

Protecting your computer from viruses and other malicious programs is not a one-time operation. Your PC needs to have security patches applied as necessary and must run antivirus software with definitions updated at least weekly. **Soon, only PCs that are properly patched and have up to date anti-virus definitions will be allowed to connect to the university network.** To avoid interruption in network connectivity, apply updates, patches, and antivirus now.

### **Apply all OS patches to your system**

Use Microsoft's Windows Update to apply all critical patches to your system. Ideally, configure your system to automatically apply patches as they are released. Otherwise, get into the routine of checking for updates weekly.

### **Install Norton AntiVirus (NAV)**

Check your machine for viruses. If your machine is infected with a virus, run a cleaning tool. Removal tools for Blaster, SoBig, and Welchia are available on [isweb.fdu.edu](http://isweb.fdu.edu). If you are unsure if you have an infection, running all the removal tools cannot hurt your computer. Companies such as Symantec have programs to remove other viruses as well.

Norton AntiVirus is provided to current students free of charge. The software can be downloaded from the [isweb.fdu.edu](http://isweb.fdu.edu) website. **IMPORTANT:** Before installing this version of Norton AntiVirus, remove all other antivirus software first, including other Symantec antivirus products.

Even with regular updates of definitions, a weekly full scan is recommended. Setting up a weekly scan is easy to do when using NAV.

For more information on backing up to the network drive, or to CD-RW, please visit [isweb.fdu.edu](http://isweb.fdu.edu). ■

## Multimedia Services

### *Multimedia Services*

Fairleigh Dickinson University's Multimedia Services Department offers full video production services to the University community seeking the creation of media to support promotional, archival, and educational projects and presentations. Multimedia Services also offers a wide array of post-production, authoring, and distribution options, from creating DVD to CD-ROMs as well as media for downloading or web streaming,

Fees associated with these services vary according to project complexity and are routinely less costly than outside vendors. Utilizing the in house capabilities of Multimedia Services for video production and duplication services ensures a level of quality, adherence to FDU standards, requirements, and mission, cost containment, and assures the protection of one of the most important university assets – the FDU brand.

Reproduction of CD/DVD's is limited to non-copyrighted material or media in which FDU owns the intellectual property.

For more information on multimedia services and charges, contact Bill Doran, Multimedia Specialist, at [wdoran@fdu.edu](mailto:wdoran@fdu.edu). ■

## CALENDAR OF EVENTS

START OF SPRING 2005 SEMESTER  
JANUARY 24, 2005

SPRING RECESS  
MARCH 14 – 18, 2005

TECHNOLOGY REFRESH  
SUMMER 2005  
Approximately 300 new computers will be deployed into the graphics labs and select staff locations.

For comments and suggestions about this newsletter, please contact Jim Lebo at [jlebo@fdu.edu](mailto:jlebo@fdu.edu)

## Did you know?

- You can visit the Telephone and Voice Services section at <http://isweb.fdu.edu> to find information on dialing instructions, voicemail and directory services. Watch for details about a new and improved voice response system coming soon.
- All students that have a Novell account are granted 5MB of network storage.
- Graduate and undergraduate students can use Webadvisor to register for classes on-line, including add/drop.
- Students are given 200 pages of free laser printing per semester.
- Soon, only PCs that are properly patched and have up to date anti-virus definitions will be allowed to connect to the university network. Be sure your system is current with operating system patches and updates and anti-virus definitions.
- The OIRT website, [isweb.fdu.edu](http://isweb.fdu.edu), contains useful information on personal computing policy and guidelines, news and security alerts, spam, ad ware, spy ware, downloads, lab schedules, helpdesk, Webadvisor and much more. This resource is available to you 24x7.
- Students and staff can create a Novell account using a web interface and without the need to visit an academic computing center. The URL is <https://neptune.fdu.edu>.
- More and more surveillance cameras are being deployed throughout our campuses to help protect our community and university assets.
- Last year, the UTAC handled almost 20,000 support requests from the university community.
- Over 57 million Americans have received 'phishing' email. Many were duped.
- During the regular semester, our computer labs are open over 85 hours a week.
- OIRT manages over 7,500 data connections.
- It takes over 30 student workers to keep the computing labs open and operational. ■

**“They key to getting ahead is getting started.”** *Mark Twain.*