http://www

JAG Wire

January/February 2009
Volume 1 Issue 3

UNT Dallas Campus Information and Instructional Technology DAL1 201R
7300 Houston School Rd Dallas, TX. 75241 http://untdallas Email: untdit@unt.edu Ph: 972.780.3626

Inside This Issue

Note to Faculty and Staff: Please remember to log off your computer daily so your files can be backed up.

"I just found out that the brain is like a computer. If that's true, then there really aren't any stupid people. Just people running DOS."
Author Unknown

10 Tips for Wireless Home Network Security

By Sameer Siddiqui, Information Technology Help Desk Consultant

Wireless networks utilize radio waves and/or microwaves to maintain communication channels between computers. Wireless networking is a more modern alternative to wired networking that relies on copper and/or fiber optic cabling between network devices. A wireless network offers advantages and disadvantages compared to a wired network. Advantages of wireless include mobility and elimination of unsightly cables. Disadvantages of wireless include the potential for radio interference due to weather, other wireless devices, or obstructions like walls.

1. Change the Default Administrator Password on Wireless Access Points and Routers:

Nearly all wireless access points and routers allow an administrator to manage their Wi-Fi network through a special **administrative account**. This account provides complete "super user" access to the device's configuration utilities with a special **username** and **password**.

See Wireless Home Network Security on page 2

EagleConnect Replaces Eaglemail

By Dr. Elizabeth Hinkle-Turner, Student Computing Services Manager

Beginning in the spring of 2009, all UNT students will be moving to a new digital communications system replacing the existing Eaglemail email-only system. This is an exciting development for the students and for the university as a whole because it greatly expands the way various members of the UNT community manage online information and communication. While the Eaglemail system only featured email communications, the new EagleConnect will allow for email, chat, calendaring, text-messaging, and online student storage as well as ever-evolving new features and capabilities.

EagleConnect is powered by Microsoft Live@EDU - a solution that centers around the 'Exchange Labs' offering best described as 'Outlook for Students'. This is significant for UNT because the faculty, staff, and students will all be on the same kind of digital message system technology allowing for many communication possibilities such as shared address books, shared and published calendars, email, and chat. Some of these features will be implemented immediately while some will come in on a more gradual schedule. The CITC helpdesk, the "Student Tour" site and a variety of other places will be keeping students up-to-date on current and upcoming features as they are put into place. Extensive tutorials will be available via the CITC Helpdesk website and the my.unt.edu portal and an example of this documentation is published in *Benchmarks Online*, December 2008, by CITC Helpdesk manager Richard Sanzone.

See EagleConnect Replaces Eaglemail on page 5

Wireless Home Network Security from page 1

Manufacturers set both the account username and password at the factory. The username is often simply the word **admin** or **administrator**. The password is typically empty (blank), the words "admin," "public," or "password," or some other simple word.

To improve the security of a Wi-Fi network, you should change the administrative password on your wireless access point or router immediately when installing the unit.

2. Turn on (Compatible) WPA / WEP Encryption

All Wi-Fi equipment supports some form of *encryption.* Naturally you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Therefore you may need to find a "lowest common denominator" setting.

3. Change the Default SSID

Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. When someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring wireless security on your network.

4. Enable MAC Address Filtering

Each piece of Wi-Fi gear possesses a unique identifier called the *physical address* or *MAC address*. Enable this, but also know that the feature is not as powerful as it may seem. Hackers and their software programs can fake MAC addresses easily.

5. Disable SSID Broadcast

In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. In the home, this roaming feature is unnecessary, and it increases the likelihood someone will try to log in to your home network. So disable it.

6. Do Not Auto-Connect to Open Wi-Fi Networks

Connecting to an open Wi-Fi network such as a free wireless hotspot or your neighbor's router exposes your computer to security risks; never connect to an open Wi-Fi network.

8. Enable Firewalls on Each Computer and the Router

For extra protection, consider installing and running *personal firewall software* on each computer connected to the router

9. Position the Router or Access Point Safely

Wi-Fi signals normally reach to the exterior of a home. A small amount of signal leakage outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the center of the home rather than near windows to minimize leakage.

10. Turn off the Network during Extended Periods of Non-Use

The ultimate in wireless security measures, shutting down your network will most certainly prevent outside hackers from breaking in.

Account Management System

If you forgot your password or cannot login to your computer, go to **http://ams.unt.edu** (AMS) to reset your password.

Passwords expire every 120 days. If you are having trouble logging into a website or your computer your password may be expired.

You can check your password expiration date, or set a password expiration reminder after logging in at **AMS**.

Blackboard Vista Update

UNT recommends Java version 6, Update 11 (JRE 1.6.0_11) with Blackboard Vista.

To check which version of Java you currently have installed on your PC:

1. Click on “Start”, then “Control Panel”.
2. Double click on the “Java” icon if you already have Java installed.
3. Click on the “About” tab and look for the “Version” number like “1.6.0_11”.

To download Java version 6, go to:
http://www.java.com/en/download/manual.jsp

For additional help contact the Vista Helpdesk at (940) 565-2324.

What is Identity Theft?

What is identity theft?
Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

The FTC estimates that as many as 9 million Americans have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft. The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector.

Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

How do thieves steal an identity?

Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.
Skilled identity thieves may use a variety of methods to get hold of your information, including:

1. **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
3. **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
5. **Old-Fashioned Stealing**. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
6. **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources. For more information about pretexting, click here.

What do thieves do with a stolen identity?

Once they have your personal information, identity thieves use it in a variety of ways.

Credit card fraud:
- They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.
- They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

Phone or utilities fraud:
- They may open a new phone or wireless account in your name, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

Bank/finance fraud:
- They may create counterfeit checks using your name or account number.
- They may open a bank account in your name and write bad checks.
- They may clone your ATM or debit card and make electronic withdrawals your name, draining your accounts.
- They may take out a loan in your name.

Government documents fraud:
- They may get a driver's license or official ID card issued in your name but with their picture.
- They may use your name and Social Security number to get government benefits.
- They may file a fraudulent tax return using your information.

Other fraud:
- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

How can you find out if your identity was stolen?

The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a

regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft. For more information, visit the Detect Identity Theft section.

Unfortunately, many consumers learn that their identity has been stolen after some damage has been done.

- You may find out when bill collection agencies contact you for overdue debts you never incurred.
- You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.
- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

What should you do if your identity is stolen?

Filing a police report, checking your credit reports, notifying creditors, and disputing any unauthorized transactions are some of the steps you must take immediately to restore your good name. To learn more about these steps and more, visit the DEFEND: Recover from Identity Theft section. To file a complaint, click here.

Should you file a police report if your identity is stolen?

A police report that provides specific details of the identity theft is considered an Identity Theft Report, which entitles you to certain legal rights when it is provided to the three major credit reporting agencies or to companies where the thief misused your information. An Identity Theft Report can be used to permanently block fraudulent information that results from identity theft**,** such as accounts or addresses, from appearing on your credit report. It will also make sure these debts do not reappear on your credit reports. Identity Theft Reports can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. An Identity Theft Report is also needed to place an extended fraud alert on your credit report.

You may not need an Identity Theft Report if the thief made charges on an existing account and you have been able to work with the company to resolve the dispute. Where an identity thief has opened new accounts in your name, or where fraudulent charges have been reported to the consumer reporting agencies, you should obtain an Identity Theft Report so that you can take advantage of the protections you are entitled to.

In order for a police report to entitle you to the legal rights mentioned above, it must contain specific details about the identity theft. You should file an ID Theft Complaint with the FTC and bring your printed ID Theft Complaint with you to the police station when you file your police report. The printed ID Theft Complaint can be used to support your local police report to ensure that it includes the detail required.

A police report is also needed to get copies of the thief's application, as well as transaction information from companies that dealt with the thief. To get this information, you must submit a request in writing, accompanied by the police report, to the address specified by the company for this purpose. You can find more information and a model letter here.

How long can the effects of identity theft last?

It's difficult to predict how long the effects of identity theft may linger. That's because it depends on many factors including the type of theft, whether the thief sold or passed your information on to other thieves, whether the thief is caught, and problems related to correcting your credit report.

Victims of identity theft should monitor financial records for several months after they discover the crime. Victims should review their credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft.

Don't delay in correcting your records and contacting all companies that opened fraudulent accounts. Make the initial contact by phone, even though you will normally need to follow up in writing. The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem.

What can you do to help fight identity theft?

A great deal.

Awareness is an effective weapon against many forms identity theft. Be aware of how information is stolen and what you can do to protect yours, monitor your personal information to uncover any problems quickly, and know what to do when you suspect your identity has been stolen.

Armed with the knowledge of how to protect yourself and take action, you can make identity thieves' jobs much more difficult. You can also help fight identity theft by educating your friends, family, and members of your community. The FTC has prepared a collection of easy-to-use materials to enable anyone regardless of existing knowledge about identity theft to inform others about this serious crime. To learn more, click here.

For more information about Identity Theft visit http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html.

If you do believe your identity has been stolen, immediately report it to the FTC by going to https://www.ftccomplaintassistant.gov/

EagleConnect Replaces Eaglemail from page 1

A new communication solution for UNT students

The final launch of EagleConnect represents the culmination of an 18-month process for choosing and implementing a new communication solution for UNT students. The timeline below illustrates some of the main highlights of the process which involved faculty, staff, and student input:

- **Spring 2007** – Student Computing session of the IT Peer Review Team brings initial call for investigating alternative digital communications solutions for the students to the current Eaglemail solution.
- **Spring/Summer 2007** – Survey conducted of the general student population regarding digital communication habits and solutions. Associate Deans' Council campus wide forum on communicating with students held.
- **Fall 2007** – Student Email Task Force convened.
- **Winter 2008** – Microsoft Live@EDU chosen as student digital communications system solution. Product is called Exchange Labs (Exchange for students – identical to faculty/staff system).
- **August 2008** – SkyDrive portion of Live@EDU rolled out. SkyDrive is the online document storage part of EagleConnect.
- **Fall 2008** – Timeline for remaining parts of EagleConnect finalized and online documentation and instructions created in preparation for the spring semester 2009.

Rollout of the EagleConnect system will be measured, with care taken to give users plenty of time to migrate from Eaglemail to EagleConnect. Tools and/or instructions to use the new system are provided and actually, many students are already using part of it by storing documents on the SkyDrive, web-based online storage solution. The timeline for the move is currently scheduled as follows:

- **January – February 2, 2009** - Students begin receiving notices of new system and implementation timeline in preparation.
- **February 3, 2009 (13th class day)** – launch date: Students told system is live now and to migrate now. Instructions and tutorials posted on using new system and migrating to new system. Full scale notification campaign begins. Current Eaglemail users given notice of the deadline for moving to new system and migrating current Eaglemail holdings to new system.
- **May 18, 2009 (Monday after spring graduation)** – Currently proposed shutdown date for turning off Eaglemail.

New format for student email addresses

The new format for student email addresses is **FirstnameLastnamePossibleNumber@my.unt.edu** (ex. ElizabethJones@my.unt.edu, JohnSmith03@my.unt.edu). Students who already receive Eaglemail through the euid@unt.edu (xyz0001@unt.edu) format or custom email address (fredsmyth@unt.edu) will not have to worry about losing touch - email will continue to come to this old address format as well. This new format is also the login name for other EagleConnect services but students will be able to use the same password that they use for their EUID. Students will be able to get their login name/new format email address from their my.unt.edu portal and through a variety of other links.

Stay tuned ...

EagleConnect (Microsoft Exchange Labs for students) works well using Outlook or a web-based interface (Firefox, Internet Explorer) on Windows machines and using Entourage (Macintosh), Safari (Macintosh), or Firefox (Macintosh and Linux). Stay tuned as we greet the 2009 New Year as the Year of EagleConnect! Any questions regarding this new system should be directed to Elizabeth Hinkle-Turner (ehinkle@unt.edu).

"Sometimes when you innovate, you make mistakes. It is best to admit them quickly, and get on with improving you other innovations."
Steve Jobs

Software Training

The UNTD IIT Department offers the following Microsoft Office 2007 training sessions monthly to the UNT Community:

- Blackboard Vista: 1st Monday
- Excel 2007: 2nd Tuesday
- Word 2007: 3rd Thursday
- PowerPoint 2007: 4th Tuesday

Additional topics are offered as requested.

To sign up for a training session, email untd.training@unt.edu.

For additional training resources, visit Microsoft Office Online:
http://office.microsoft.com/en-us/training/FX100565001033.aspx

Software Tips

Check Your Style in Word 2007

First, Word could check your spelling, and then your grammar; now it can even critique your writing style. If you're concerned about things like wordiness and improper use of the passive voice, have Word 2007 check for them. Click the **Office button > Word Options > Proofing**. Under **Writing Style**, select **Grammar & Style** from the dropdown. If there are particular areas you don't Word to scrutinize, click the adjacent Settings button and then uncheck the appropriate boxes.

Show Page Breaks in Excel 2007

Printing an Excel spreadsheet can be a hassle, but you don't need to go to Print Preview in order to see where a page breaks. Click the Office button, then under Excel Options, click Advanced. Under "Display options for this worksheet" click the box next to "Show page breaks."

Change Your Presentation's Resolution in PowerPoint 2007

With larger wide-screen displays becoming the PC-viewing norm, you might not want your PowerPoint presentation to go online formatted for an old-school 800x600 resolution. To bump up your presentation's optimal screen size, click the **Office button > PowerPoint Options > Advanced**. Under the **General** area, click **Web Options**, select the **Pictures** tab, and choose the screen size you want.

Open Multiple Web Sites in Internet Explorer 7

Want IE to open two or more tabs when you start it up? Go to Tools > Internet Options, then type as many addresses as you want (on individual lines) in the "Home page" field.

Dim the display to save power on your laptop

A laptop's biggest battery-life-sucking component is its LCD display. To eke out more juice when you're off the plug, turn down your panel's brightness to the lowest level your eyes can stand. Most notebooks have a Function key combo—or even a dedicated hot key—for a quick crank-down. (You can also adjust brightness in Display Settings under Control Panel.)

Keyboard Shortcuts for Windows

Windows Key+U+U
Quickly shut down Windows by hitting the Windows key (don't hold it down), hitting U to reach the shutdown menu, and then hitting U again to shut down.

Ctrl+Z, Ctrl+Y
Undo an action by hitting Ctrl+Z; if you change your mind, Ctrl+Y will redo the undo.

Shift + Arrow Keys
Holding shift and pressing one of the arrow keys will highlight text in Word (or a group of Excel cells) without the mouse, selecting in the direction the arrow points.

Sudoku Puzzle

3		7						
4		9	7		1	3		5
				3			8	
				4			6	
2		4	1		6	5		3
1		5						
	3		6					9
7		1			9	8		
	2		3					1

University of North Texas Dallas Campus
Information and Instructional Technology

7300 Houston School DAL1 201R
Dallas, TX. 75241

Phone: 972.780.3626 **Fax:** 972.780.3696

E-mail:
untdit@unt.edu

"Give a person a fish and you feed them for a day; teach that person to use the Internet and they won't bother you for weeks."
Author Unknown