

COPYRIGHT & FILE SHARING: WHAT YOU NEED TO KNOW



File-sharing itself is not illegal; it's the files that are traded that cause problems. You may trade any information that is not protected as freely as you want: just like photocopying something that is not protected, but when you trade copyright protected material, you are breaking the law.

"Colleges and universities have become prime targets for copyright owners who fear whole sale theft of

their wares. Because institutions of higher education typically have higher bandwidth capacities than commercial Internet service providers, higher concentrations of potential purchasers of music, games, and videos than the population as a whole, and college students are more easily identifiable than teenagers connected via commercial ISP's, it seems that the copyright owners make special efforts to track down illegal sharing of files on college campuses."

-Dr. Maurice Leatherbury, Associate Vice President for Computing and Chief Technology Officer, University of North Texas



PHYSICAL SECURITY

Physically protect your sensitive information from thieves by following these simple tips:

- Always shut down or log off of any system when not in use.
- Protect your computer from power surges by using a surge protector; and protect it from power loss by using a UPS (Uninterruptible Power Supply).
- Use password-protected screensavers.
- Make sure no one is looking over your shoulder when you enter your password.
- Lock your doors when you leave your office.
- Never lend your key to anyone.
- Find out who has access to your work area and computer.
- Shred all documents that contain sensitive information when they are no longer needed (social security numbers, grades, bank account statements, etc.).
- Never carry Social Security information or card numbers.
- Never leave sensitive information (personal information, passwords, etc.) in plain view
- Never leave valuables unattended (Laptops, PDA's, books etc.).

MORE INFORMATION

For more information about security, read the Information Security Handbook for Faculty, Staff, and Students:

<http://www.unt.edu/security/handbook>

For information about UNT computing resources visit the CITC Helpdesk website:

<http://www.unt.edu/helpdesk>

To report a computer security incident, email: secu-



Computing and Information
Technology Center

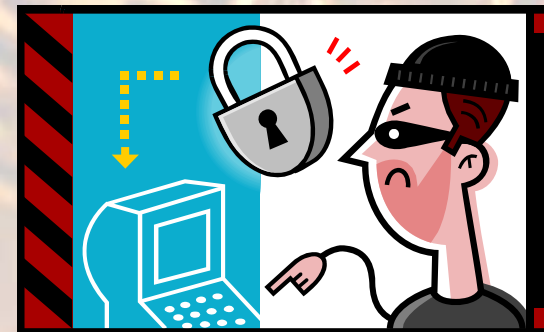
Take these simple steps to significantly decrease the chances of being the target of a hacker. Visit

<http://www.unt.edu/security>
for more information, or email
security@unt.edu

©2005 University of North Texas
PS50495-8/04i
Revised 07/05

IS YOUR COMPUTER SECURE?

UNIVERSITY OF
NORTH TEXAS



Learn how to protect yourself from becoming the next victim of a computer crime.

Brought to you by the
University of North Texas
Computing & Information Technology Center
Information Security Team
www.unt.edu/security
& Helpdesk

WARNING!!!

If you do not take proper precautions, you will be at risk for a hacker to break into your computer or steal your personal information. A hacker that breaks into your computer can do many things that can harm your

computer. That long report you stayed up until 4AM researching/typing – deleted. The project you've been working on all semester that's due tomorrow – deleted. Don't take the "it won't happen to me approach." Help protect your information and your computer by implementing a few

EUID & PASSWORD SECURITY

Passwords are your first line of defense. Choose a good password and use these simple tips to help provide increased security.

- Use a mnemonic, such as the first letter of a song verse or a phrase, while adding in numbers, symbols (\$,%,*), and UPPER/lower case letters to help you remember that complicated password you just created.
- If it's in any dictionary – it's a bad password: don't use it!
- Select a password that is a minimum of six characters (preferably eight) in length.
- Change your password often!
- Never write down a password and never share accounts.
- Do not give your password to anyone, not even the Help-desk!
- Never share or grant access to your account to anyone.
- Never use your EUID or password for non-UNT systems.

EMAIL TIPS

Email is an easy target for attackers. Use these tips to help protect your computer and your information.

- Never open an email attachment or click on links from strangers! Ever! Not even 'this once!'
- Never forward chain letters or hoaxes. They tie up email systems.
- If someone you know sent you an email attachment that you weren't expecting, do not open it without first talking with the sender: His/her computer may have a virus!
- Never respond to spam (Unsolicited email) or click "remove me from mailing list" links—often that will just add you to a list to receive more spam.
- Never respond to email solicitations requesting 'verification' or requesting personal information: this is likely a fraud or an

VIRUS & WORM PROTECTION

Protect your computer from viruses and worms. See below for more information.

- UNT students are eligible for a **free** copy of McAfee Antivirus.
- To download your free copy, or for instructions on setting up McAfee Antivirus, go to <http://www.unt.edu/security/virus>.
- You may also purchase an inexpensive copy in the UNT bookstore.
- Install it, use it, and most of all **update** it daily to be protected from the latest virus and worm threats.

COMPUTER HOAXES AND BACKUPS

- Beware of computer hoaxes. You can find a list of the top 10 recent hoaxes on our website <http://www.unt.edu/security>.
- Backup important information: Burn a CD, or take advantage of UNT's Student Storage. Visit <http://untss.unt.edu/> for more information.

SYSTEM PATCHES AND UPDATES

If you are using a Microsoft Windows operating system, go to <http://windowsupdate.microsoft.com> to check for the latest updates. The service will automatically tell you what updates you need.

Also, Microsoft has a similar website for Microsoft Office updates: <http://update.microsoft.com>

To automate Windows XP Updates: Right click "My Computer", select "Properties", click "Automatic Updates" tab, select "Automatic".

If using a Mac operating system, reference the software update feature for the latest updates.

If using a Linux based operating system check that developers' website for system patches.

Also, visit the websites of other companies whose software you are running on your computer to find any available patching information. Not only will this help make your computer more secure, it can make it more stable.

Keeping your computer up-to-date is one of  your

ARE YOU BEING SPIED ON?

When you install certain programs (such as file-sharing programs or shareware software) on your computer, you are usually (unknowingly) installing multiple spyware or adware programs as well. Spyware is a program that gathers information about you and what you do on your computer without you ever having knowledge of it, and then sends the information to different sources. Along with raising many privacy concerns, spyware can also be a big nuisance to your computer, severely slowing it down and possibly causing frequent crashes. Adware may also be unknowingly installed on your computer causing multiple pop-up advertisements.



IDENTITY PROTECTION INFORMATION

- Before purchasing anything on the web or providing any personal information (bank account number, credit card number, etc.), always make sure that the webpage is secure. Look for <https> in the web address (Notice the 's'). This shows that the website is using encryption.
- Email is not an appropriate method for sending confidential information, as most email providers do not provide encryption.
- Solicitations for private information about you is a tactic known as "Phishing". These emails are often disguised as emails from a bank or financial institute. Never provide them with confidential information or click on links or attachments.
- Avoid using debit cards for online transactions.
- Obtain free credit report from the three main credit bureaus at least once a year. Contact your bank for more information.
- Review your bank and credit card account statements regu-

APPROPRIATE USE AND PRIVACY

The University of North Texas provides computing resources for the purpose of accomplishing tasks related to the University's mission.

- Unauthorized use of UNT computing resources is prohibited.
- Use of UNT computing resources is subject to review and disclosure in accordance with the Texas Public Information Act and other laws.
- You have no reasonable expectation of privacy in regard to any communication or information stored on a UNT computer system.
- Use of UNT computing resources constitutes your consent to security monitoring and testing and administrative review.
- Use of UNT computing resources must be limited to justifiable computing support of UNT activities in accordance with [UNT Policy 3.10: "Computer Use Policy"](#) and [UNT Policy 3.6:](#)