Identity Theft Protection

Identity theft is a major concern in today's digital world. But, by following a few steps, you can greatly reduce your chances of becoming a victim of identity theft:

- Avoid sending confidential or personal information via email, as email can often be relatively easily intercepted by unauthorized individuals.
- When visiting websites where you intend to shop or provide personal information, always make sure your computer's connection to the website is secure (encrypted). To determine if a website is secure, the beginning of the web address will include "https://" and will often include an image of a padlock icon.
- When shopping online, always check the reputation of the website you are visiting. If there are complaints about the website, shop elsewhere.
- Watch for unauthorized purchases charged to your credit and debit cards. If you believe your card or card number has been stolen, contact your card provider to resolve the issue and cancel the card immediately.
- Review your credit report at least once a year. Obtain a report from each of the three major credit bureaus. This way you can detect if any unauthorized transactions have been made in your name without your permission.
- For more information about identity theft, visit https://itss.untsystem.edu/security/identity-theft.

Human Resources Security

All employees must understand their roles and responsibilities pertaining to information security.

- New employees must receive information security awareness training and be informed regarding security policies and procedures prior to being granted access to information resources.
- All staff must complete annual information security awareness training.
- Upon termination or change of employment, all confidential and proprietary information and information resource assets must be returned to the organization as per designated exit procedures.

Working Remotely

In order to work remotely, an employee must first obtain approval from their supervisor. Any device used to access information resources remotely must be up-to-date and utilizing antivirus software. Once these requirements have been met, an employee can access resources remotely by connecting to https://vpn.unt.edu.

For additional help using the VPN, contact your department IT support staff or helpdesk.

More Information

For more information about security, read the Information Security Handbook and the Information Security Users Guide.

https://itss.untsystem.edu/security/guidelines-laws-and-regulations

For information about computing resources at UNT institutions visit the following website:

https://security.untsystem.edu

Additional Resources

For additional information, including information about policies, laws, and the Security Handbook, please go to:

https://itss.untsystem.edu/security/guidelines-laws-and-regulations

If You've Been Compromised

If you feel that your information or your computer has been compromised, please contact the Help Desk

UNT UIT Helpdesk: http://www.unt.edu/helpdesk

UNT Dallas Helpdesk: http://dallas.unt.edu/iit/help

UNT System Service Desk: ithelp@untsystem.edu or 940-565-HELP (4357)

If confidential or sensitive data is associated with any computer involved in the incident, please contact Information Security immediately at 940-369-7800 or security@untsystem.edu

Refrain from accessing or further interacting with the computer in question. This will help preserve evidence integrity before the Information Security team can collect an image for forensic analysis.

Recipient:

©2016 UNT System

IS YOUR COMPUTER SECURE?

Information Security Brochure For Employees

Image ©2016 Cody Abbott

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

UNT SYSTEM™
IT Shared Services

Brought to you by the
UNT System
IT Shared Services
Information Security Team

Cyber-attacks do happen, but they don't have to happen to you. By following just a few tips for good practice, you can drastically minimize your risk of attack as an employee.

EUID and Password Security

A strong password is your first line of defense against attack.

- Consider using a passphrase. Build your password from a phrase you know and can remember. For example, starting with the phrase "Safe and Secure", you could create "S4f3&s3cur3!" This is both relatively easy to remember and incredibly difficult for an attacker to guess. (NOTE: Please do not use this specific password.)
- Always use passwords that are a minimum of 8 characters, including capital and lowercase letters, and numbers. Remember—longer passwords are much less likely to be guessed by an attacker!
- Avoid using dictionary words, your EUID, your name, or any other identifiable information in your password.
- Never save, write down, or share your password.

Email, Phishing, & Social Engineering

The availability of information on social media is attractive to attackers.

- Be careful when responding to or clicking a link in an email that asks you to verify an account or reset a password. If the email appears to be from a reputable source, but you weren't expecting it or it looks suspicious, contact the reputable source by some other means and verify they sent the email.
- If you receive an email with an attachment you weren't expecting, don't open it. These attachments could be infected with malicious code, such as a virus or a worm. Even just opening a document or PDF can be enough to infect your computer or device.
- When in doubt, notify Information Security at security@untsystem.edu of any suspicious email. It is always better to be safe than phished!
- Remember—no one should EVER ask you to tell them your password. If you receive such a request, report it to Information Security immediately.

Malware Protection

A major line of defense for all employees to protect their computers and devices is utilizing antivirus software, and always keeping it up to date. Doing so will maximize your computer's ability to avoid becoming infected with malware.

Students, faculty, and staff with a valid EUID and password can download a free copy of McAfee Antivirus. Go to https://itss.untsystem.edu/security/antivirus-download to get your free copy.

Backing Up Your Important Information

Hardware and software failure occasionally happens, but you can minimize the impact of failure by keeping backups of your important files.

- While working on a document or other type of file, save your work often.
- Save backups in a secure location.
- If possible, save your work to your university OneDrive account. These drives are automatically backed up to multiple locations, making files recoverable and secure.
- If you need to perform your own backup, contact your IT manager for assistance.

Disaster Recovery & Business Continuity

Disasters can strike at any given moment. Adequate plans must be in place to address how every department would operate in the event of either a natural or technological disaster that could potentially cause an outage to services. It is important to have a plan in place that addresses how critical operations would continue to operate if enterprise services became unavailable.

For more information, please email drbcp@untsystem.edu.

Copyright, Software Licenses, & File Sharing

Sharing or distributing copyrighted files is illegal. Examples of copyright protected files include music, movies, and other materials. Sharing files that are not protected by copyright is acceptable. Copyrighted materials may be used under the terms of fair use as noted in US copyright laws.

Follow the requirements and limitations of software licenses. Read the license agreement! Users caught violating copyright laws or software license agreements may face disciplinary action.

Protecting Confidential Information

It is your responsibility to protect any confidential information that you come into contact with from unauthorized use or disclosure. You must receive permission from information owners to obtain and use confidential information. Confidential information can include any information that would not be generally made available to the public, such as organizational secrets, financial statements, medical records, credit card numbers, and personally identifiable information. Any portable device that contains data or information that is considered confidential must be encrypted.

Contact your Helpdesk or IT Manager to learn more about encrypting confidential information.

Physical Security

Physical security is just as important as digital security. Follow these steps to ensure your devices and information remain physically protected from unauthorized use:

- Always use a password protected screensaver, or set the lock screen on your computer or device when not in use.
- Always lock your office door when the office is empty.
- Avoid allowing unauthorized persons to work in an office unsupervised.
- Avoid leaving valuables unattended.
- Avoid lending your keys to anyone.
- Make sure no one is looking over your shoulder when accessing sensitive data or typing your password.
- Make sure you know the rules for disposing of information and documents before doing so. Follow the requirements of the records retention schedule.
- Always use a surge protector or UPS (Uninterruptable Power Supply—also called a Battery Backup) to protect your computer or device from a power surge. Power surges can result in loss or damage to equipment connected to the device.
- If you notice an unauthorized person in a secure area, report the person to your supervisor or other persons in authority.

Appropriate Use

Always follow the requirements of the information security policy when using computer resources owned by your institution. These policies can be found at https://itss.untsystem.edu/security/guidelines-laws-and-regulations.

Please note:

- Unauthorized use of computer resources is prohibited.
- Use of a computer resource 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 university owned computer.
- Use of a university owned computer resource constitutes your consent to security monitoring and testing, as well as administrative review.

System Patching and Updating

You should always keep your system and software current and up to date. If possible, set your software to update automatically. This will ensure that any security holes that are found in the software will be patched, making your system more secure. If you are told you need to update or restart, schedule a time to do so to ensure that your computer will always have the latest security applied.