System Patching and Updating

Keep all personal devices and their software current and up to date. If possible, set the software to update automatically. This will ensure that any security vulnerabilities that are found in the software will be patched, making the device more secure. If a device indicates that an update or restart is needed, schedule a time to do so to ensure that the device will always have the latest security applied.

Malware Protection

A major line of defense for protecting a computer or other devices is utilizing antivirus software, as well as keeping it up to date. Doing so will maximize a 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 for Windows or Mac. Go to https://itss.untsystem.edu/security/antivirus-download to get your free copy.

Backing Up Your Important Information

Hardware and software failures occasionally happen, but the impact of a failure can be minimized by maintaining regular backups of important files.

- While working on documents or other files, save often.
- Save backups in a secure location.
- If possible, save to a cloud-based location such as your university OneDrive account. These drives are automatically backed up to multiple locations, making files recoverable and secure.

Using Public Wi-Fi

When using an unfamiliar Wi-Fi network, such as the Wi-Fi at a coffee shop or hotel, it is always best to add an extra layer of protection to prevent others from seeing your online activities. Use a Virtual Private Network, or a VPN. All students, faculty, and staff can use the UNT System VPN located at https://vpn.unt.edu to access their files if stored in a UNT system.

To setup and use the UNT System VPN, please follow the steps outlined in the UNT System Campus VPN Guide available at https://itss.untsystem.edu/sites/default/files/campus_vpn.pdf.

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

UNT SYSTEM
IT SHARED SERVICES

If You've Been Compromised

If you feel that your personal computer has been compromised or infected, your computer should be taken to a trusted IT Professional. Then, using a different computer that you know is safe, change any passwords that might have been entered into the compromised computer.

Keep in mind that prevention is your best option, and repair may result in complete loss of data!

Remember:

- NEVER share your password with anyone!
- ALWAYS update the software on your computer!
- ALWAYS run reputable, up-to-date antivirus!
- ALWAYS back up your most important files!
- ALWAYS protect your connection when using free, public Wi-Fi!

IS YOUR COMPUTER SECURE?

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

For Students

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, you can drastically minimize your risk of attack.

EUID and Password Security

A strong password is the first line of defense against attacks.

- Consider using a passphrase. Build your password from a phrase you know and can remember. For example, starting with the phrase "Safe and Secure", a user might create "S4fe&s3cur3!" as a password. 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.
- Avoid setting security questions whose answers can be found online or on social media.

Appropriate Use

Always follow the requirements of the information security policy when using university computer resources. This policy can be found at https://itss.untsystem.edu/security/guidelines-laws-and-regulations.

Please note:

- Unauthorized use of a university owned computer resource is prohibited.
- Use of a university owned 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.

Email, Phishing, & Social Engineering

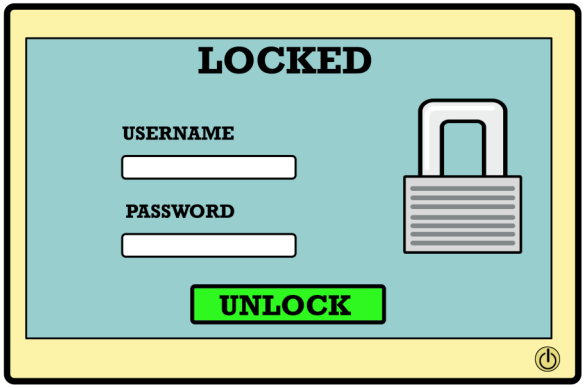
Always keep in mind that the amount of personal information available on social media is attractive to attackers.

- 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 that 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.
- Remember - no one should EVER ask you to tell them your password. If you receive such a request, delete the message immediately.

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.
- 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.
- 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.



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.

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 personal information via email, as email can often be relatively easily intercepted by unauthorized individuals.
- When entering personal information online, make sure your connection is secure (encrypted). Always look for "https://" at the beginning of the web address, and, often, a locked padlock icon to the left of the web address.
- Watch for unauthorized purchases charged to your credit and debit accounts. Contact the account provider if you notice unauthorized activity.
- For more information about identity theft, visit https://itss.untsystem.edu/security/identity-theft.