

Policy and Procedure

UT Arlington faculty, staff, and students are expected to abide by all applicable information technology policies, including:

UT Arlington Policy
www.uta.edu/policy

UT System Policy
www.utsystem.edu/policy

Texas Administrative Code 202
www.sos.state.tx.us/tac

Family Educational Rights and Privacy Act (FERPA)
www.ed.gov/policy/gen/guid/fpco/ferpa

Digital Millennium Copyright Act (DMCA)
www.copyright.gov/legislation/dmca.pdf

Federal Copyright Laws (Title 17)
www.copyright.gov/title17

Network Monitoring

The UTA Information Security Office has network monitoring software and devices in place that allow the monitoring of inbound and outbound network communications.

All unauthorized use is prohibited and misuse is subject to criminal prosecution. Usage may be subject to security testing and monitoring. There is no expectation of privacy except as otherwise provided by applicable privacy laws.

University administration will provide any evidence of illegal computing activities to appropriate law enforcement officials.

Software Patches

Patches are regularly released to update your operating system and software. It is especially important to keep your operating system up to date. Microsoft updates are made available through Microsoft Windows Update or at windowsupdate.microsoft.com. Apple updates are available through the "Update Software" function of the operating system. Linux updates are made available through the package manager provided with your operating system.

VPN

If you need to connect an off-campus computer to a resource on the UT Arlington network, a VPN (virtual private network) client must be installed. This client creates a secure tunnel between the remote computer and the campus network; this allows information to pass over the internet in an encrypted state. For more information on this service, visit www.uta.edu/vpn.

MavSpace

MavSpace is a secure online storage and file sharing service provided to all faculty, staff, and students. To access MavSpace or for more information visit mavspace.uta.edu.

Contact Us

www.uta.edu/security
blog.uta.edu/security
security@uta.edu
817-272-5487

SECURE

Revision Date: 8/2010

INFORMATION SECURITY OFFICE

Computer Security
Starts with



Social Engineering

Social engineering is a method in which an attacker attempts to solicit information that could be used for malicious purposes. An attacker may use email, phone or in-person visits to gain information.

- * Never divulge sensitive information or information about UTA computers or networks.
- * Always ask to see an official UT Arlington ID card if someone comes to your office to work on your computer.
- * Do not leave sensitive information lying out on your work desk; always lock important documents away.
- * Never insert or connect an unknown USB drive, CD, DVD, or device to your computer; this might contain malware.

If you suspect that you have become a victim of social engineering, call the Information Security Office immediately at **817-272-5487**.

Spam and Phishing E-mail

Phishing emails attempt to persuade the recipient to reveal personal information, like passwords or bank account numbers. UT Arlington will never ask for your password and neither will any other reputable entity. If you receive an email and are unsure about the legitimacy, call the sender of the email.

- * Never click on links in an email—always type the web address into your browser.
- * Never respond to spam or phishing emails.
- * Consider creating a separate e-mail account to sign up for newsletters and advertisements to reduce the number of spam messages you receive at your primary email addresses.
- * Only use your UT Arlington email address for official University business.

Password Security

Your password is your first line of defense! Always use a password that is:

- * At least 8 characters long.
- * Uses at least three character classes (lowercase letters, uppercase letters, numbers, or special characters).
- * Is not the same as any of your last 5 passwords.
- * Does not contain any part of your NetID.
- * Is not based on a word found in the dictionary.

Never share your password with anyone and do not write it down.

You are required to change your password once every six months. However, it is recommended that you change it more frequently.

Be sure to visit www.uta.edu/selfservice to setup your personal NetID identification questions. This can save you valuable time should you forget your password and need to change it.

Anti-Virus Software

Your computer is under constant attack when you are connected to the Internet. Downloading files, opening email attachments and web surfing all expose your computer to malware.

To prevent data corruption and loss, you should always run an anti-virus program (no matter what operating system you use). Keep the program up-to-date with the latest virus definitions and make sure to set up a scan of your computer regularly (at least once a week).

Free anti-virus software is available for all current UT Arlington faculty, staff and students and can be downloaded at www.uta.edu/antivirus.

BlazeWare

Some security tools are licensed for the personal use of current faculty, staff, and students. These tools are available via BlazeWare, a software and documentation CD.

BlazeWare is updated and released typically three times a year; at the beginning of the Fall and Spring semesters as well as at the start of the Summer.

Copies are often available at Information Security events and all software is available for download on the Information Security BlazeWare webpage: www.uta.edu/blazeware.

Sensitive Data & E-mail

It is against UT System policy to transmit sensitive information via unencrypted email; this includes social security numbers and credit card numbers.

Very few offices at UT Arlington require social security numbers; the 10 digit UTA ID number is usually enough information to locate records and receive service or information.

Never email a social security or a credit card number. Should you receive an email that contains sensitive information, you must redact the information before replying.

Unauthorized Access/Theft

If you suspect that there has been unauthorized access to your computer/account or your UTA computer has been stolen, you should contact the UTA Police at **817-272-3381** and the Information Security Office at **817-272-5487** immediately.

Computer Security Starts with

