Security Best Practices

-

Never open e-mail attachments or links you don’t recognize.
Configure your junk mail settings (http://junkmail.utoledo.edu).
Never respond to spam.
Don’t provide sensitive or personal information over email where possible.
Before clicking “send”, review your message for appropriateness.

When transmitting personal information, look for https or secure (key) icon in browser to ensure data is sent encrypted.

Don’t bring software from home without authorization.
Never turn off Anti-virus or Anti-spyware programs.
Scan removable media for viruses before using.
Ensure program and operating system updates are installed regularly.

File-sharing is not illegal, but sharing copyrighted material is.
File-sharing software must be authorized before usage.
Know what your computer is sharing!
The penalties for sharing copyrighted or inappropriate material are severe.

Refrain from storing sensitive information on your University computer or laptop.
The University provides network storage space for all institutional members and departments (H drives, department shares, etc.).
If you must store sensitive information on your computer for official business purposes, you must encrypt it. Store backup copies of important files in a safe and secured location.
Storage must be appropriately wiped or erased before transfer or disposal.
Avoid using removable media (such as flash drives, USB devices, DVD/CDs, and floppies) unless required. These can easily be lost or stolen.

Use password-protected screen savers.
If screen savers are not available, cover up display when not in use.
Be aware who can read your display.
Use power-saving techniques when not in use.
Be aware of what you display during a presentation.

Get your print outs quickly. Anyone can be standing at the printer.
Don’t print excessive copies, especially if printing isn’t working as expected.
Ask for assistance if you print to the wrong printer.
Inform others when they leave print outs at the printer.
Printers should be in a secured area, or away from public access.
Dispose of all sensitive print outs in confidential bins.
You are responsible for everything you print.

Verify the caller.

Don’t disclose sensitive information without approval.

Be careful of what information is left on other’s voicemail.

Can anyone else hear your conversation?

Avoid asking for personal or sensitive information, unless required.

Contact the recipient of a fax prior to transmission.

Use fax cover sheets on all faxes and mark the transmission as “confidential”.

Remove or mask sensitive information when faxing.

Know whether the fax machine is in a secured or public area.

Don’t take patient or sensitive information home!

Don’t leave mobile devices unattended, even for a few minutes.

Don’t leave University equipment unattended in your automobile.

Secure University equipment when at your personal residence. You are responsible for protecting this equipment!

Ask for identification if someone you don’t know is in your area.

Always shut down or log off of any system when not in use.

Protect your computer from power surges with surge protectors.

Use locks where possible.

Lock your doors when you leave your office and never lend your key to anyone.

Know who has access to your work area and computer.

Properly dispose or shred all documents that contain sensitive information when they are no longer needed.

Never leave sensitive information in plain view.

Never leave valuables unattended (Laptops, PDA’s, books, etc.).

Always secure sensitive documents when not in use.

Always empty desks and cabinets before transferring ownership.

Review & understand the University’s Responsible Use of Information Technology Policy (www.utoledo.edu/policy/index.asp?id=68), which includes:

Complying with All Federal, State, and University laws.

Computing resources are subject to review and disclosures.

Using University systems provides your consent to security monitoring, testing and administrative review.

Respect the privacy of other users and their accounts.

Refrain from using any UT computing resource for personal commercial purposes.

Use only the UT computing resources that you are authorized to use.

Users that violate this policy may subject to penalties and disciplinary action, both within and outside of the University.

Communications made with University resources are generally subject to Ohio’s Public Records Statute.