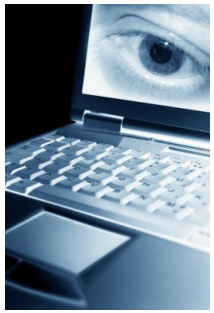
i.t.solutions Security Services

Encryption Software for Laptops

If you keep any sensitive information on your laptop, or if you are a frequent traveler, get the Check Point Full Disk Encryption software that is available as a service to faculty and staff. If anyone gains physical access to your computer, the typical hacker's tools cannot access the data on your disk with this encryption.



Departmental Vulnerability Assessments

Is your department vulnerable to attack? If you have a group of PCs you wan to secure, consult with i.t.solutions staff to conduct vulnerability assessments. We will identify and correct vulnerable system configurations and missing patches, and detect any existing malware or spyware. The process may take more than an hour per system, but knowing that you are safe is worth it. The assessment meets operating system and network standards for security.

Virus Removal

Even careful people can get hacked—we can help.

Contact TAG to coordinate any of these services.

Free Antivirus Protection on the UAHuntsville Network!

One of the first lines of defense in the cyber security combat zone is a good antivirus package that is updated frequently to protect against the newest viruses. As a service to the UAHuntsville community and as a means of self protection, UAHuntsville has contracted with McAfee to provide the latest **McAfee VirusScan Antivirus** software free of charge for faculty and staff and users of the campus wireless.

To obtain the software you can download it from http://www.uah.edu/itsolutions/software.php when you are connected to the UAHuntsville network.

Additionally, **McAfee's ePO Agent** is employed on Faculty and Staff workstations to keep antivirus definitions up to date.

Contact TAG if you need antivirus assistance.

Technical Assistance Group (TAG)

E-mail: tag@uah.edu
Phone: 256-824-3333

i.t.solutions
uahuntsville

E-mail: itsolutions@uah.edu
Web: http://its.uah.edu

National Cyber Security Awareness Month

Cyber Safety 2011 : Faculty Staff Edition

A guide to i.t.solutions security services and data protection

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Keep Our Data Safe

Are you keeping sensitive information secure? Are you taking steps to protect university information? Safeguarding sensitive data in your files and on your computers is just part of being a good campus citizen. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft.

What you can do ...

Your approach to data security should be based on four key principles:

Take stock — Know what sensitive information you have in your files and on your computers.

Scale down — Keep only what you need for your job.

Lock it — Protect the information in your care.

Pitch it — Properly dispose of what you no longer need.

What needs to be protected ...

Federally Protected Data

- Family Educational Rights and Privacy Act (FERPA) protected information (e.g., student information and grades)
- Health Insurance Portability and Accountability Act (HIPAA) protected information (e.g., health, medical, or psychological information)
- International Traffic in Arms Regulation (ITAR) restricted software

UAHuntsville Proprietary Data

Research and other proprietary information of the university

Personal and Financial Data

- Social Security number (SSN)
- Credit card number or banking information
- Tax information
- Credit reports
- Anything that can be used to facilitate identity theft (e.g., mother's maiden name)

What malware can do ...

Mess with your protection

- Prevent signature updates on installed antivirus and antispyware tools
- Disable antivirus and anti-spyware tools to prevent identification and disinfection
- Pretend to be an antivirus or antispyware tool that actually plants some spyware or virus

Mess with your privacy and data

- Capture keystrokes to detect login and activity at a financial services or e-commerce website
- Gather the information you input into forms to get account and authentication information (form scraping)
- Turn on your camera, microphone, or even video camera and violate your privacy and personal space
- Intercept and control sensitive documents
- Inject specific advertisements into your search results

Use your system for bad

- Install spyware programs that can install and execute other spyware (cascading file-dropper)
- Relay spam from your machine unbeknownst to you
- Install spyware that allows an attacker to control your system remotely (bot)
- Monitor network traffic for user IDs and passwords on systems near your machine (sniffer)