

Security Awareness


SECURITY AWARENESS

Security Issues

<http://its.uah.edu>

Security Items for 2010

- Passwords
- Social Networking
- Phishing
- Anti-virus
- Confidential Data
- Protection of Mobile Confidential Data
- Incident Reporting
- Backup
- Computer Disposal & Information Destruction
- Patch Management
- Regulatory Compliance (FERPA, HIPAA, PCI)



Passwords

L922M0102

- Password Paradox: use a strong password and remember it.
- Password strength depends on:
 - Length
 - Complexity
- Strong password have the following characteristics:
 - At least 8 characters long
 - At least one alphabetic character
 - A mix of upper and lower case characters
 - At least one numeric character
 - At least one special character
- Passwords should be mobile. Change them often, and do not use the same password for all of your accounts.
- Screen savers should be password protected.

- Dangers of Social Networking
 - Phishing and Identity Theft
 - Loss of Privacy
 - Viruses and Malware
 - Cyberbullying
 - Other Predators
- How to be safe while networking
 - Keep private information private!
 - Use privacy settings.
 - Only approve friend requests from those you know.
 - Only post info you are comfortable with others seeing.
 - Always make sure you are at the REAL site when entering your credentials.
 - Have a healthy skepticism.

Phishing is type of fraud, usually carried out electronically using eMail, Instant Messaging, or Text Messaging. It seeks to steal private information (such as passwords or bank account/credit card numbers) by posing as a trustworthy party or organization.

- Never reply to an unsolicited email that asks for personal information.
- Never click on any links within an unsolicited eMail.
- It is against UAH Acceptable Use policy to share account information/passwords.
- Always use common sense and good judgment.



Antivirus

- According to PC World, there were more than 25 million strains of malware identified in 2009 alone
- Users should ensure that their systems have up-to-date antivirus and antispyware software
- The software must be configured to update automatically
- When you access files from external devices or import attachments, you should scan the documents for malicious code
- ePO managed systems are automatically updated and are configured to scan for malicious code automatically on local and external devices
- The UAH Software Agreement with McAfee allows employees and students to utilize the antivirus software for both Windows and Macintosh systems for home use

Generally, confidential data is any information that contains the following elements in conjunction with an individual's name or other identifier:

- Social Security number
- Credit card number
- Driver's license number
- Bank account number
- Patient treatment information

Research Data



Protection of Mobile Confidential Data

PROTECTION OF MOBILE CONFIDENTIAL DATA

- Laptop
 - Enable Passwords
 - Hard Drive and USB flash drive encryption
 - Secure with cables when possible

- Phone
 - Enable screen password
 - Flash storage cards and SIM cards can hold sensitive data
 - Remote wipe is available for select phones



Incident Reporting

When to report an incident:

- You suspect unauthorized use of your Chargernet, email, or network accounts
- You suspect unauthorized use of university computer assets
- Your university-owned laptop, desktop, or mobile device was lost or stolen
- You want to report other stolen university computer assets
- You suspect potential unauthorized access to, or disclosure of, university confidential data (SSN, Research, credit card)
- You have computer security questions or concerns
- You suspect that you have a virus, worm or some other type of malware

What to do:

- If you are working on a system where you suspect there has been unauthorized access: stop all work!
- Report all incidents to your supervisor
- Contact ITS Security
 - Call TAG Service Desk to open a ticket. (256) 824-3333
 - Or send an email to tag@uah.edu.



Backing Up Your Data

BACKING UP YOUR DATA

- It is important that you backup critical information on your system
- Is your data backed up? Are you sure?
- What to back up? Examples: My Docs, Email, Photos, internet favorites, media, etc.
- Contact your local IT support or TAG service desk for backup options
- External drives i.e. USB flash drive or hard drives
- “Cloud” or Internet Storage
- Mobile phone backups? Blackberry, iPhone, Sync often!

Computer Disposal and Information Destruction

- Prior to disposal or reuse, computer systems should be sanitized and secured
 - Confidential data can remain “hidden” on old hard drives and may not be cleaned off by the system’s new owner
 - Wiping hard drives ensures that research data, confidential University data, or personal data is destroyed
 - Contact TAG Service Desk for assistance
- Be aware of any confidential data that you store on external storage like USB Flash Drives, DVDs, CDs, and external hard drives
 - Destroy unwanted media to ensure they are secured
 - Use ActiveKill or KillDisk to wipe external hard drive storage
 - Use Eraser to wipe a single file

- Most security incidents are caused by flaws in software (vulnerabilities)
- According to CERT statistics, the number of vulnerabilities reported has increased exponentially over the years (from only 171 in 1995 to more than 7,200 in 2007)
- Patches are the ultimate solution to software vulnerabilities
- Backup your system and files periodically
- Keep your system patched
- Keep both the applications and operating system up-to-date

- Basic security training should be attended annually
- Additional compliance training should be attended as follows:
 - If you use patient treatment data or have access to a facility that contains patient treatment information: HIPAA annual training and acknowledgement
 - If you use student records of current students: FERPA training
 - If you process credit cards for customers: PCI

- Security is everyone's responsibility....

J. Ashley Ewing, CISSP, CISA

University of Alabama

ashley.ewing@ua.edu

(205) 348-6524