http://its.uah.edu

OCTOBER 2010

NATIONAL CYBERSECURITY AWARENESS MONTH

WORKSTATION SECURITY RISKS

Take the following precautions at your workstation.

- Do NOT use third-party IM software — Try Google Talk
- Do NOT use Facebook without proper privacy settings
- Do NOT allow the browser to store passwords at login
- Do NOT use the administrator account for day to day work
- Do NOT click on popups claiming to be antivirus protection
- Do NOT open email attachments, download shareware, or visit web sites from questionable sources
- Do NOT use insecure Remote Desktop connections
- Do NOT ignore regular back-ups
- Do NOT fail to add password protection to your screen saver

i.t.solutions
uahuntsville

http://its.uah.edu

NATIONAL CYBERSECURITY AWARENESS MONTH OCTOBER 2010

SECURE WORKSTATION BEST PRACTICE

The following are safe practices at your workstation.

- Install antivirus software, keep it current, and scan weekly
- Stay up-to-date on Windows, MS Office, Adobe Reader and Flash, Sun Java and other installed applications
- Use Firefox with Ad-Block and NoScript, or Google Chrome — if you must use it, upgrade Internet Explorer to 8.0
- Browse with Web of Trust (WOT) safe browsing tool
- Clear cache & files with CCleaner and run malware scans
- Use strong passwords and change them often
- Turn off file and print sharing
- Use SSH instead of telnet and FTP
- Turn off USB autorun
- Lock your PC when you leave your desk

i.t.solutions
uahuntsville