http://its.uah.edu

OCTOBER 2010

NATIONAL
CYBERSECURITY
AWARENESS MONTH

UAHuntsville

WIFI SECURITY-THINGS NOT TO DO

Take the following precautions when connecting to a public wireless hotspot.

- Do NOT connect to unsecure or unknown WiFi networks
- Do NOT pay bills, access bank accounts, or use credit cards
- Do NOT store login and password information when prompted by your browser for sites that have sensitive information like banks or credit card companies
- Do NOT leave a wireless card active when its not in use
- In Windows 7, do NOT Select anything but Public Network when setting a network location —
  Public Network blocks file & print sharing and turns off network discovery, which can also be disabled in MAC OS X

i.t.solutions
uahuntsville

http://its.uah.edu

OCTOBER 2010

NATIONAL
CYBERSECURITY
AWARENESS MONTH

UAHuntsville

WIFI SECURITY-THINGS TO DO

The following are safe practices when connecting to a public wireless hotspot.

- Ask the concierge or barista the official name of the establishment's WiFi — rogue wireless is often available
- Select a secure WiFi network, indicated by a lock and requiring a password to connect
- Use a VPN
- Stay up-to-date with antivirus software, applications, and your operating system
- Connect only to secure websites when accessing sensitive information (https:// secured with SSL)
- Use encryption software

i.t.solutions
uahuntsville