7 PRACTICES FOR COMPUTER SECURITY

1. Protect your personal information. It's valuable.
2. Know who you're dealing with.
3. Use security software that updates automatically.
4. Keep your operating system and Web browser up-to-date, and learn about their security features.
5. Keep your passwords safe, secure, and strong.
6. Back up important files.
7. Learn what to do in an emergency.

For more information visit Onguard Online at http://www.onguardonline.gov/

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 students, users of the campus wireless and faculty/staff computers. To obtain the software you can download it from http://www.uah.edu/tag/ when you are connected to the UAH network.

A second tier of defense, McAfee's ePO Agent, is also available to Faculty and Staff at UAHuntsville.

Contact the TAG Help Desk at 256-824-3333 for assistance.

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

How To Be Cyber Safe

NATIONAL CYBERSECURITY AWARENESS
OCTOBER 2010

it solutions
uahuntsville

Email: itsolutions@uah.edu

Web: http://its.uah.edu

Staying Safe Online

The web seems almost as vital to life as water. When was the last time you have gone three days without some kind of access to the Internet? But just as contaminated water can be harmful, there are risks associated with accessing online resources.

GENERAL PRECAUTIONS

Protect Your Social Security Number — Sharing it is like handing over the keys to your identity.

Protect Your Privacy — Know what information the site is collecting and how it is used. Find out if they are sharing information. When filling out forms, enter only required information; leave optional fields blank.

Keep Passwords Private — Never share your passwords, change them frequently, and do not use the same password for multiple sites. Don't display or store passwords on or near your PC.

Don't Email Personal/Financial Information — UAHuntsville and other reputable institutions will NEVER ask you to send passwords or other secure information via email.

Trust Your Instincts — If it doesn't feel right, don't do it. Be skeptical to a fault.

Look Over Your Shoulder — Always be aware of your surroundings and make sure that no-one in the real world can snoop into your online space.

SHOPPING AND INVESTING

Know Your Merchant — Before placing an order with a vendor, check the Better Business Bureau, seller ratings, and the site's privacy, security, and return policies. Make sure there is an alternate contact number in case something goes wrong.

Only Use Secure Websites — Shop and invest only on sites that offer an https:// connection. Another indicator that you are using a secure website is a padlock or unbroken key.

Only Use a Credit Card — With a credit card you have the right to dispute charges, which is not available with a debit or check card, bank checks, or cash. It is also a good practice to use a single credit card for all of your online ordering.

Keep Good Records — Print your order and check against your credit card statement

to ensure that your account was not used without permission.

Only Shop on a Secure Connection — Never do online shopping or banking at a public kiosk or from an unsecured wireless network.

SOCIAL NETWORKING

Don't Share Too Much — Be careful about how much personal information you post, including vacation plans

Use Privacy Settings — Be mindful of privacy settings and keep informed of new features that may affect your privacy,

Know your Friends — Do not accept friend invitations from strangers.

Post Nothing That Will Prevent You From Getting a Job or Running for Office — Don't say anything or post any pictures that you wouldn't show your great-grandma.

Do Unto Others — Do not engage in cyber bullying or forwarding other people's embarrassments, as you would not want that to happen to you. Respect and reciprocate the privacy of others.

Do Not Meet Friends You Make Online — The person you are talking to may not be who you think. If you do meet an online friend, do not go alone.

Make Sure You Are on the Real Social Network — Beware of phishing sites disguised as a social networking site that can capture your login and wreak havoc on your account.