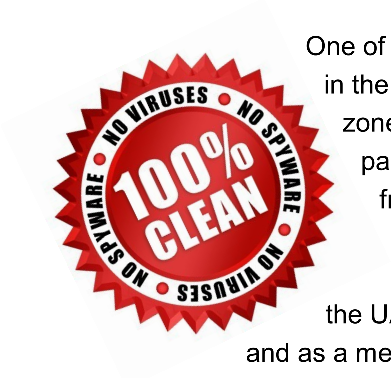
The DMCA and YOU …

The Digital Millennium Copyright Act (DMCA) is a United States law that was passed in 1998 to prosecute illegal digital use of copyrighted material. A DMCA notice is a third-party legal notification, typically from an artists association. It provides the copyrighted piece (s) in violation and a link to settle. If you do not comply, you can be fined or sued. Universities are required to distribute DMCA notices to offending network users.

Peer-to-peer (P2P) technology is the primary mechanism for violating the DMCA. P2P activity occurs when you make a portion of your computer resources directly available on the network. The DMCA criminalizes P2P activity because it circumvents measures that control access to copyrighted works.

Any time you use P2P programs (BitTorrent, Ares, BearShare, Gnutella, Kazaa, Limewire, eMule, etc.), you are in violation of UAHuntsville network policy. When this activity is detected, you will be disabled from using the UAHuntsville network. However, use of these programs is dangerous on any network. If you receive a DMCA notice from UAHuntsville or any other internet service provider, you are at risk. Keep money in your pocket (to legally use on iTunes or Amazon) by NEVER using P2P software.

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 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.

Contact TAG if you need antivirus assistance.

Technical Assistance Group (TAG)

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

it
i.t.solutions
uahuntsville

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

National Cyber Security Awareness Month

Cyber Safety 2011 : Student Edition

A guide to staying safe, private, and legal on the UAHuntsville network and the Internet

UAHuntsville
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

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? Just as contaminated water can be harmful, however, 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.

Be Careful When You Click— Ads, popups, and downloads can contain viruses. Take extra caution with those designed to look like antivirus software.

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.