Students

If you are a college student, you are probably immersed in the world of information and communications technology. That makes you a digital citizen, with both rights and responsibilities for staying safe online and helping to keep others safe as well. (http://www.staysafeonline.org/content/top-cyber-security-practices)

Cyber Security

A computer's Internet connection is like a gate that swings both ways: allowing files, software, pictures and information of all kinds both in and out. That in-and-out flow is the reason we use the Internet: receiving and sending information keeps us in touch with friends and family, allows us to meet new people, exchange ideas, conduct research, make purchases, and learn about any topic under the sun. But there are also some dangers to the in-and-out. All users should be aware of these dangers and take precautions to prevent damage.

What's coming in?

By accessing the Internet—from your own desktop, a university computer, or a laptop at a coffee shop—you open a potential window for all sorts of nasty stuff: viruses, worms, Trojan horses, spyware, phishing e-mails, spoof, and corrupted files can all wreak havoc on your system, and through your system on those of others with whom you exchange e-mails, files, or other communications.

To protect your computer, your files, and those of your friends, schoolmates, and others with whom you communicate, it's critical that you install the three core protections (http://www.staysafeonline.org/content/top-cyber-security-practices-tip?page=4) on your computer—anti-virus, anti-spyware, and firewall software—and keep them up to date.

In addition to these tools, your own behavior can help keep you safe. Do not open e-mails from unknown sources, and treat all files acquired over the internet as potentially infected. It is up to you to keep your "door" to the Internet locked, and only open it when you are sure of the safety of what you're letting in.

What's going out?

Remember that the gate swings both ways: harmful files and programs can come into your system, but what flows out from your computer can also put you in danger. Treat personal information such as credit card numbers, bank accounts, your social security and student ID

numbers, phone number, and private photos with caution. Whether you provide them in response to a request or post them voluntarily, these items in the wrong hands can cause more than just headaches: giving away too much information online can lead to financial, emotional, and even physical harm. So before sharing information online, think about it:

If personal or private information is being requested by an unknown party or web site, think WWW:

- **Who** wants this information?
- **What** information are they asking for?
- **Why** do they need it?

Do not share any information unless you are satisfied with the answers to all three questions. And if you are considering posting pictures or video of yourself, your friends, or your enemies on social networking sites such as Facebook or Myspace or sharing these images via text message, take a moment to consider whether they could damage reputations or create bad feelings if they got into the wrong hands—say, those of a potential employer, a past or future dating partner, or even the media. Thanks to the wonders of YouTube, homemade videos of "youthful indiscretions" can easily ruin careers, relationships, and lives. Think twice before you post or share—once it's "out there" there's no getting it back.

Cyber Safety

Staying safe online is not just about protecting information and reputations. Sometimes it's about protecting yourself or others physically as well. People you meet online *and* people you already know in "real life" can use cyberspace as a tool to perpetrate abuse, harassment, and stalking. In many cases, people who commit "cyber stalking" and "cyber bullying" do not confine their actions to the cyber world, but use a mix of online and in-person techniques to cause their victims fear, embarrassment, and other emotional and sometimes physical harm.

To minimize your risk of being harmed by a cyber stalker or cyber bully, use both tools, like the core protections (http://www.staysafeonline.org/content/free-security-check-ups), and behaviors, such as taking online relationships into the real world only with caution, meeting online acquaintances in public places and letting friends know where you are and when you'll be back.

For more information on reducing your risk of victimization by cyber stalkers or cyber bullies and what to do if you've already been harmed, see the National Center for Victims of Crime's Stalking Resource Center www.ncvc.org/src, Wired Safety's www.stopcyberbullying.org, or the FTC's www.OnGuardOnline.org.

Cyber Ethics

Each computer user is a potential victim and a potential threat to others' cyber security and cyber safety. Do your part to surf ethically by committing to the following principles:

- **No flaming.** When you participate in online forums, discussion groups, or other communications, consider the repercussions of tossing verbal bombs. If you wouldn't say it to someone's face, don't say it online. And if you're the sort of person who would verbally abuse someone to their face, consider getting some help for that problem.

- **Respect others' intellectual property,** including copyrights, trademarks, licensing agreements, and other legal protections. Unauthorized downloading of music, videos, software, and other copyrighted material is not only illegal, it's taking the product of someone else's work without fair compensation. Put yourself in the shoes of someone who created something and offered it for sale hoping to make a profit (or a living), only to find others giving it away for nothing. Not cool. Sharing, copying, or downloading unauthorized copies of files or software also exposes your system to possible viruses.

- **Properly cite information found online (and find good information).** The Internet has made research immeasurably easier than it was for college students a generation ago. But the quick and easy availability of information also means that students have to learn to discriminate good information from bad, reliable sources of information from questionable ones. You can find tips on how to do this at http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/Evaluate.html. When you do find good information and use it in your school work, be sure to follow the rules for properly citing the information in your research papers. For information on how to cite online sources in APA format, click here (http://www.nova.edu/library/dils/lessons/apa/).

Today's college students are vital links in the chain of our nation's cyber security. The National Cyber Security Alliance encourages all students to be a part of the solution by adopting good habits in the areas of cyber security, cyber safety, and cyber ethics.