



NATIONAL CYBERSECURITY AWARENESS MONTH

National Cyber Security Awareness Month: Our Shared Responsibility What College Students Can Do

When you're in college, your computer and mobile device are primary tools in your educational and social life. Many students use the Internet for homework, research, social networking, online purchases, and more. The Internet is an amazing tool, but must be used safely and securely. Consider doing the following during National Cyber Security Awareness Month:

Educate Yourself

Basic Cybersecurity and Online Safety

- **Pack it up:** Take your laptop with you, even if you intend to be right back. Unattended laptops in public places such as the library, study lounge, and coffee shops are an invitation for theft or unwanted access to your information.
- **Protect your passwords:** If you need to write them down, keep them in a secure location away from your computer. Don't keep any passwords in your laptop case or on a piece of paper stuck to the laptop. Never share your passwords with anyone.
- **Use different passwords for all online accounts:** Secure passwords are long and complex (are at least 9 characters, include numbers and symbols, are NOT single words, pet names, birthdays, etc).
- **Back up your computer files:** Computers can be compromised, stolen, or destroyed in an accident or natural disaster. Make electronic copies of your files regularly so you don't lose important assignments, cherished music, or photos. Keep backed up files in a safe, secure location away from your computer. Consider using an online service.
- **Use caution on wireless networks:** Be careful which sites or services you access when using public wireless networks. Even if they're secure (i.e. require a password), you never know who else is using the network.
- **Secure your own wireless networks:** If you have your own wireless network, secure access by requiring a long, complex password. Change the password frequently, such as at the beginning of each term.
- **Be sure your personal laptop or computer has the security software tools you need:** anti-spyware, anti-virus, and a firewall, all set to update automatically. Keep your operating system and Web browser up-to-date as well.



NATIONAL CYBERSECURITY AWARENESS MONTH

- **Be cautious when using public computers**, such as those in hotels or computer labs. Don't visit sites that require personal information, such as your bank's Web site, and be sure to log off when you're done.
- **Turn your computer off when it's not in use:** This saves electricity, preserves your laptop battery, and protects you from hackers that try to access your information through wireless networks.
- **Learn more at www.staysafeonline.org.**
- **Become a fan of NCSA's Facebook page at www.facebook.com/staysafeonline.**

Social Networking

- Be cautious about how much information you provide on social networking sites like Facebook and Twitter. The more information you post, the easier it may be for a hacker to use that information to steal your identity or access your data.
- Learn about and use the privacy settings on social networks.
- Protect your reputation on social networks. What you post online stays online – forever. Think twice before posting pictures you wouldn't want your parents or future employers to see.
- Limit your social network to “real” friends: people you know, trust, and want to keep up-to-date about your activities. If you're trying to create a public persona as a blogger or expert, create a separate profile.
- If a friend posts something about you that makes you uncomfortable, let them know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable.

Online Shopping and Banking

- Whether you're buying textbooks or a ticket home for the holidays, limit online shopping to merchants you know and trust. For those you don't, conduct online research to see how other consumers have rated them.
- Pay for online purchases with a credit card or an online payment service. These methods of payment limit your liability if something goes wrong.



- Keep a paper trail of purchases and check your credit card and bank statements regularly.
- Look for indications that a Web site has taken extra security steps when conducting online transactions (for example, a Web address that begins with “https” or “shttp”).
- Don’t provide financial information, including credit card, bank account, or Social Security numbers through email. Only send information over Web sites whose URL address begins with “https” or “shttp.”
- Before you share personal information, ask yourself WWW:
 - Who’s going to see it?
 - What’s the value of it?
 - Why do they need to see it?

Downloading and File-sharing

- Be wary of free downloadable software and file-sharing programs. They often contain malware that can steal your information or harm your computer. Music, video and game files on these sites are often pirated, and could put you in violation of copyright laws. If caught, you could be subject to stiff penalties, including fines and prosecution.
- Be alert to phishing scams in email and on Web sites. Attempts to collect your personal information or requests for immediate action are indicators that you are being phished. These include notices of account closures, disconnection of service, request for immediate verification of account information, etc. Even though some may look legitimate, they could be scam emails (made to look like they come from a real business). A bank will NEVER request your account information via email. If you’re uncertain, directly type in the web site address of the site into your URL bar. You can also call your service provider, but use the number given on your account statement, not the one given in the email.
- Don’t follow email links or pop-up ads that claim your computer is infected and offer anti- spyware software. These could be what is known as rogue anti-spyware programs and may actually contain spyware.



NATIONAL CYBERSECURITY AWARENESS MONTH

Educate Your Friends

- Post a link to the NCSA's Top Tips (available at www.staysafeonline.org/top-tips) on your social networking site.
- Contact the school webmaster and ask them to post cybersecurity tips or a link to www.staysafeonline.org on the school's Web site.
- Print out NCSA's Cyber Security Awareness Month poster (available at www.staysafeonline.org/content/posters-and-more) and hang it in your dorm, sorority or fraternity common areas.
- Print out NCSA's Top Tips brochure (available at http://www.staysafeonline.org/files/NCSAM/PalmCard_FINAL.pdf) and distribute it through student groups, dormitory and Greek system.
- Organize a presentation about basic cybersecurity for your student organization, dorm, sorority or fraternity.

