National Cyber Security Awareness Month: Our Shared Responsibility

What College Students Can Do: Educate Yourself

Basic Cybersecurity and Online Safety

1. Pack it up and take your laptop with you, even if you intend to be right back. Unattended laptops in public places like the library, study lounge, and coffee shops are an invitation for theft or unwanted access to your information.
2. 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.
3. Use different passwords for all online accounts. Secure passwords are long and complex (at least 9 characters, NOT single words, pet names, birthdays, etc.) and include numbers and symbols.
4. Back up your computer 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 (or use an online service).
5. Be careful which sites or services you access when using public wireless networks. Even if they're secure (require a password to get on), you never know who else is using the network.
6. 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.
7. Be sure your personal laptop has the security software tools you need: a suite of security software, operating system, and web browser all set to update automatically.
8. Use caution 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.
9. Turn your computer off when it's not in use. This saves your battery (laptops), protects you from somebody accessing it, and saves electricity.

Social Networking

1. Be cautious about how much personal information you provide on social networking sites like Facebook, MySpace, 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.
2. Learn about and use the privacy settings on social networks.
3. 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.

4. 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, more open profile and limit personal information there.
5. If a friend posts something about you that makes you uncomfortable or you think is inappropriate, 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

1. 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.
2. Pay for online purchases with a credit card or an online payment service. These methods of payment limit your liability if something goes wrong.
3. Keep a paper trail of purchases and check your credit card and bank statements regularly to be sure that you're the only one spending your money.
4. "Https" or "shttp" at the beginning of a Web address (URL) are each an indication that a Web site has taken extra security steps to protect your information. Look for either one when conducting online transactions.
5. Don't provide financial information, including credit card and bank account, or Social Security numbers through email. Only send information over Web sites that are "https" or "shttp."
6. 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?

Downloads and File sharing

1. Be wary of free downloadable software. This type of software often contains spyware or other malicious software that can steal your information or harm your computer.
2. Practice caution when using free file-sharing programs. These sites are notorious for distributing malicious software (malware) that can be used to steal your passwords and other personal information. 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.
3. Be alert to phishing scams in email, Web or social networking 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 in question or call your bank

or other service provider on the number you would normally contact them, not one provided in the email or Web site.
4. 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.
5. Learn more at staysafeonline.org.

Educate Your Friends

1. Share cybersecurity tips with your friends.
2. Join the staysafeonline.org Facebook group or post a link to staysafeonline.org's Top Tips on your social networking site.
3. Contact the school webmaster and ask them to post cybersecurity tips or a link to staysafeonline.org be posted on the school's website.
4. Print out NCSA's Cyber Security Awareness Month poster and hang it in your dorm, sorority or fraternity common areas.
6. Print out NCSA's Top Tips brochure and distribute it through student groups, dormitory and Greek system.
7. Organize a presentation about basic cybersecurity for your student organization dorm, sorority or fraternity.