In 2009, President Obama issued the Cyberspace Policy Review, which tasked the Department of Homeland Security with creating an ongoing cybersecurity awareness campaign—Stop.Think.Connect.—to help Americans understand the risks that come with being online.

Stop.Think.Connect. challenges the American public to be more vigilant about practicing safe online habits and persuades Americans to view Internet safety as a shared responsibility at home, in the workplace, and in our communities.
A 2011 survey conducted by the Pew Research Center’s Internet & American Life Project found that 83% of Internet users age 18 to 29 use social media, which includes a large number of undergraduate students.

FINDINGS:

- Eighty-six percent of college students actively use social media.
- How many connect via a mobile device? About 63% of undergrads log on while on the go.
- Undergraduates are much more likely to access the Internet through their mobile device than the overall population.
- Ninety-four percent of first-year undergrads engage in social media use.
SOCIAL MEDIA USE

While social media helps us stay more involved, informed and interconnected than ever before, it comes with risks.

• Many of the crimes that occur in real life are now facilitated through the Internet, including human trafficking, credit card fraud, identity theft, and embezzlement.

• Scammers increasingly use social networking sites such as Facebook, Tumblr, Pinterest, and Instagram to gather information and target victims.

• The Internet is a great place to swap pictures and make weekend plans, but keep in mind that cyber criminals are lurking; your former and future employers are finding out about you through social media; and even your grandparents may be checking up on you. What you say and do online is visible to others, and it cannot be erased.

DID YOU KNOW?

• Facebook is the most widely used social network by college students, followed by YouTube and Twitter.¹

• Students spend roughly 100 minutes per day on Facebook.²

2. Johnson & Wales University, The Effects of Social Media on College Students, 2011
SHARING INFORMATION

Criminals can use information provided in your social media profile—such as your birthday, routine, hobbies, and interests—to guess the answers to the security questions on your account or impersonate a trusted friend. Predators appreciate your help if you post your daily routine and whereabouts online.

In the News: Cyber Stalker Sentenced to Four Years in Prison
- ABCNews, January 2012

• A 24 year-old man targeted a University of Central Florida college student and is accused of sending a series of disturbing messages to her on Facebook, YouTube and Twitter.

• He harassed the victim and sent her videos demanding her affection and even threatened to kill her if she didn’t return his affection.

• After all of the messages sent to the victim, he was finally caught and sentenced to four years in prison.

• Despite the arrest, the victim stated that she will forever be affected by the incident.
YOUR ONLINE IDENTITY

Determine how you will portray yourself online—your personal brand—as information you share on the Internet becomes increasingly accessible to others. What steps are you taking to protect yourself and your identity?

- **Set Up Privacy Restrictions.** Your social media network has likely expanded to include peers and potential employers who may have access to your photos, comments, check-ins, and status updates. Spend time creating appropriate privacy settings for the various members of your network.

- **Think About Your Future.** Perform a quick search of yourself online. Do your findings represent the identity you would want a potential employer or university admissions officer to see? Consider setting up alerts for searches on different variations of your name with your school(s), place(s) of employment and other distinguishing details.

More than a third of employers use social networking sites to research potential job candidates.¹

Cyber predators are people who search online for other people in order to use, control or harm them in some way.

DID YOU KNOW?
If you divide the number of your Facebook friends by 11, the resulting number is the number of real friends that you’re likely to have.¹

TIPS:
• Keep your personal information private, including the names of your family members, your school, your telephone number, and your address.

• Think twice before you post or say anything online; once it’s in cyberspace, it’s out there forever and can adversely impact your ability to get a job later in life.

• If you think someone is contacting you under false pretenses, inform university authorities.

Identity theft is the illegal use of someone else's personal information to steal money or credit.

TIPS:
• Create strong passwords with eight characters or more that use a combination of numbers, letters and symbols.
• Don’t share your passwords with anyone.
• Lock your computer and smartphone whenever they are not in use.
• Keep social security numbers, account numbers and passwords private, as well as specific information about yourself, such as your full name and birthday.
• Don’t open emails from strangers and don’t click on links for unfamiliar sites; if you think an offer is too good to be true, then it probably is.

DID YOU KNOW
Eighteen to twenty-nine year olds issue the most identity theft complaints.
Thirty-one percent of all identity theft complaints received by the Federal Trade Commission in 2012 were filed by young adults.¹
Fraud is the intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right. Phishing is a scam by which a user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.

TIPS:

• Most organizations—banks, universities, companies, etc.—don’t ask for your personal information over email. Beware of requests to update or confirm your personal information.

• Don’t open emails from strangers and don’t click on unfamiliar sites; if you think an offer is too good to be true, then it probably is.

• Make sure you change your passwords often and avoid using the same password on multiple sites.

• It’s better to enter a new website address by typing it into the browser instead of following a link.

• Be wary of messages that encourage you to act immediately, as well as offers that invite you to join an event or group on a social networking website with incentives like free gift cards.

DID YOU KNOW?
The education sector accounted for 18% of all data breaches in 2011.¹

U.S. colleges and universities have become a favored target for phishing - 70% of those attacks target online portals of the universities which offer various student services, including webmail.²

1. A Chronology of Data Breaches, Privacy Rights Clearinghouse, June 2013
2. RSA Security, U.S Colleges and Universities Become a Favored Target for Phishing, 2009
CALL TO ACTION

Cybersecurity is a shared responsibility that all Americans must adopt in their communities in order to keep the nation secure in the 21st Century.

Become an advocate on your campus to help us educate and empower undergraduate students to take steps to protect themselves online.

How to get involved:

• Become a Friend of the Campaign by visiting [www.dhs.gov/stopthinkconnect](http://www.dhs.gov/stopthinkconnect).

• Lead or host a cyber awareness activity for your educational or social groups on campus.

• Blog, tweet or post about Stop.Think.Connect.

• Talk to your friends and family about safe online behavior.

• Volunteer within your community to mentor kids and teens on the basics of online safety.
The Stop.Think.Connect. Campaign also promotes science, technology, engineering, and math (STEM) education among students.

• To help keep our computers and our country’s networks safe, we need more cybersecurity professionals.

• To do that, we need students who have skills in science, technology, engineering, and math.

To learn more about STEM education and careers, visit the National Initiative for Cyber Careers and Studies (NICCS) Portal at http://niccs.us-cert.gov/.
YOU HAVE A SHARED RESPONSIBILITY TO KEEP THE INTERNET SAFE
• Email us at: stopthinkconnect@dhs.gov.

• Download student resources at: http://www.dhs.gov/stopthinkconnect.

RESOURCES AVAILABLE TO YOU…

• StopBullying.gov: Find out what to do if you or someone you know is being bullied.

• iSafe.org: Become an iMentor and promote cyber safety awareness in your home, school and community.