STOP.THINK.CONNECT.™

National Cybersecurity Awareness Campaign

Undergraduate Student Presentation

Homeland Security

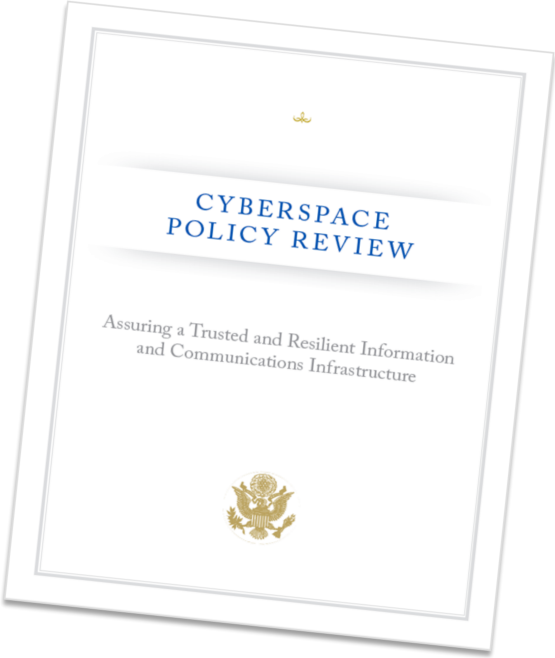
STOP | THINK | CONNECT™

STOP.THINK.CONNECT.™

About Stop.Think.Connect.

- 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** home, in the workplace, and in our communities



CYBERSPACE POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

National Cyber Security Awareness Month

Homeland Security

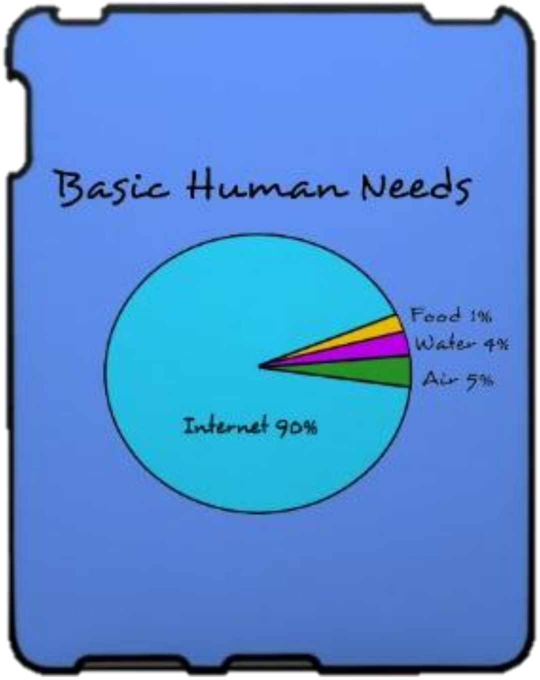
STOP | THINK | CONNECT™

24 Hours: Unplugged

A 2010 study from the International Center for Media & the Public Agenda (ICMPA) at the University of Maryland asked 200 students to give up all social media links (laptops, mobile phones, etc.) for 24 hours

Findings:

- Most college students are not just unwilling, but **functionally unable to be without their media links to the world**
- Students used terms associated with substance addictions to describe how they felt about "unplugging": ***In withdrawal***, ***Frantically craving***, ***Very anxious***, ***Extremely antsy***, ***Miserable***, ***Jittery***, ***Crazy***
- 18-21 year old college students' lives are wired together in such ways that **opting out of that communication pattern would be renouncing a social life**



STOP.THINK.CONNECT.™

Social Media Use

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

- Many of the crimes that occur in real life are now done - or at least facilitated - through the Internet. Human trafficking, credit card fraud and identity theft, embezzlement, and more – all can be and are being done online
- The Internet isn't a boundless cyber-playground to swap pictures and make weekend plans. Cyber criminals are lurking; your former and future employers are surfing the web to find out more about you; even your grandparents may be checking up on you. What you say and do is visible to others, and it's not erasable

Did You Know?

- Facebook is the most used social network by college students, followed by YouTube and Twitter[1]
- Students spend roughly 100 minutes per day on Facebook[2]

[1] Nielsen Media Research
[2] Online PhD

STOP.THINK.CONNECT.™

Sharing Information

Criminals can use information provided about a person's birthday, routine, hobbies, and interests to impersonate a trusted friend or convince the unsuspecting that they have the authority to access personal or financial data.

Predators appreciate your help if you post your daily routine and whereabout s online

In the News: Sorority pledges tormented by Facebook predator

-MSNBC, December 2010

- A 27 year-old Florida man targeted Louisiana State University college students on Facebook by posing as a sorority sister, sexually harassing them and threatening violence
- Victims were contacted through Facebook by someone claiming to be an alumna of the sorority they were pledging, using fake names that included "Marissa" and "Lexie"
- The same predator is suspected in cyber stalking investigations by police at the University of Florida, Florida State University, Auburn University, the University of Alabama, and University of Tennessee

Your Online Identity

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

- **Set-up Privacy Restrictions.** Your social media network has likely expanded to include peers and managers who might have access to your photos, comments, check-ins, and status updates. Take the time to set up the appropriate 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 education admissions office 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

56% of companies use social media sites to screen potential job candidates[1]

[1] Society for Human Resource Development

Cyber Predators

***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]

"On the Internet, nobody knows you're a dog."

Tips:

- Keep personal information about yourself private, including your family members, your school, your telephone number, or your address
- Think twice before you post or say anything online; once it is in cyberspace, it is out there forever
- If you think someone is contacting you under false pretenses, inform university authorities

[1] The Future Laboratory

STOP.THINK.CONNECT.™

Identity Theft

Did You Know

- **18 - 29 year olds** issue the most identity theft complaints
- **24%** of all identity theft complaints made to the Federal Trade Commission are made by college students

Identity theft *is the illegal use of someone else's personal information in order to obtain money or credit*

Tips

- Don't use the same password twice
- Choose a password that means someone to you and you only
- Lock your computer and cell phone
- Don't share personal information without knowing exactly who is on the receiving end. Use strong passwords that are hard to guess and don't share them with anyone other than your parents
- 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

Homeland Security

Source: Federal Trade Commission

STOP | THINK | CONNECT™

STOP.THINK.CONNECT.™

Fraud & Phishing

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 an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently*

Did You Know?

- The education sector accounted for **21%** of all data breaches last year[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]

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
- Always enter a URL by hand instead of following links

Homeland Security

1. Open Security Foundation
2. RSA Security

STOP | THINK | CONNECT™

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 Americans to take steps to protect themselves online*

How to get involved:

- Become a *Friend* of the Campaign by visiting **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
- Consider a career in cybersecurity if you enjoy science, technology, engineering or math

STOP.THINK.CONNECT.™

YOU have a *shared responsibility* to keep the Internet safe