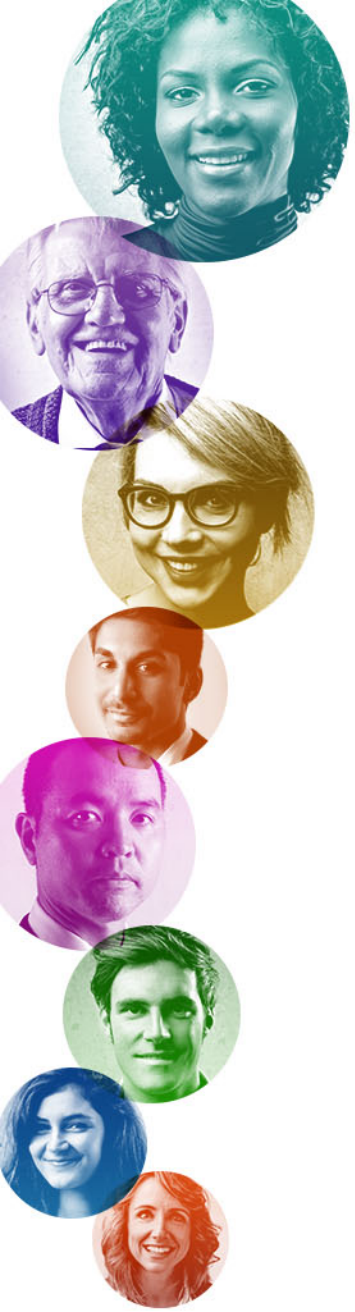
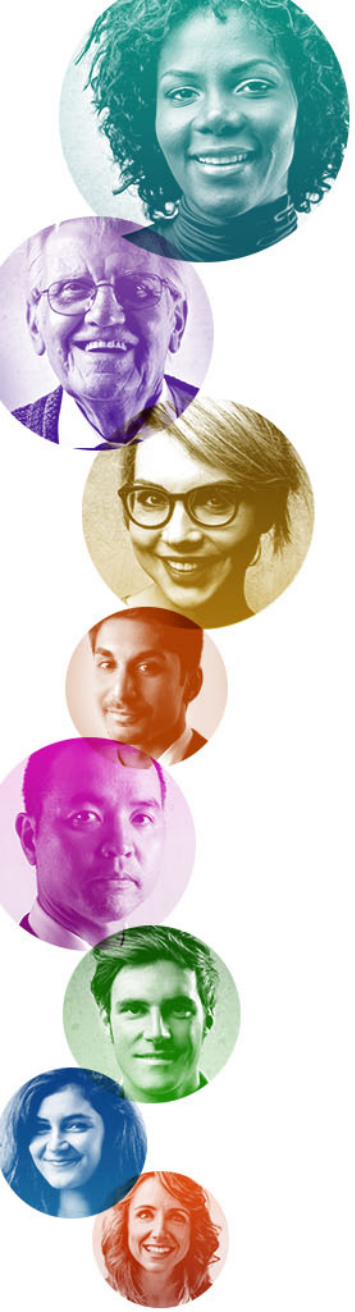

STOP.THINK.CONNECT™
NATIONAL CYBERSECURITY AWARENESS CAMPAIGN
UNDERGRADUATE STUDENT PRESENTATION
Homeland Security
STOP | THINK | CONNECT™



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.

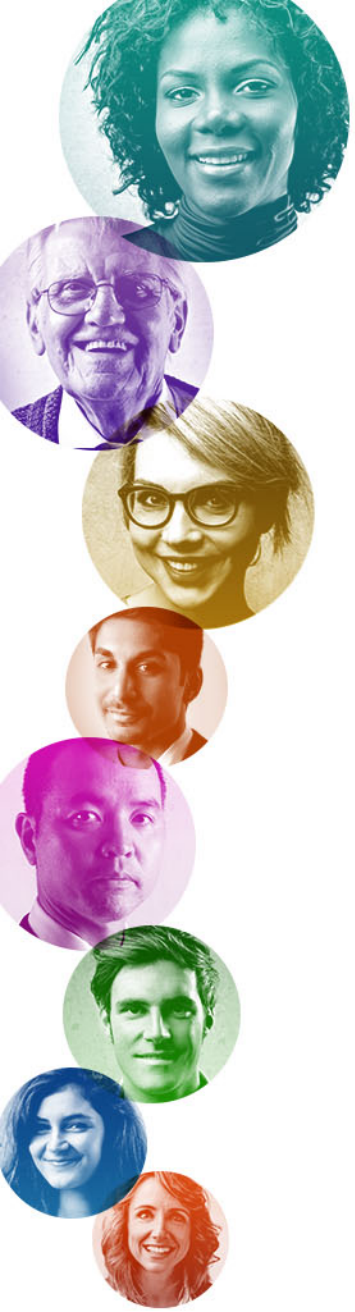
Stop.Think.Connect. challenges the American public to be more vigilant about practicing safe online habits and persuades Americans to view Internet safety as a **shared responsibility** at home, in the workplace, and in our communities.



YOUNG ADULTS AND THE INTERNET

*A 2011 survey conducted by the Pew Research Center's Internet & American Life Project found that **83%** of Internet users ages 18 to 29 use social media.*

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.



SOCIAL MEDIA USE

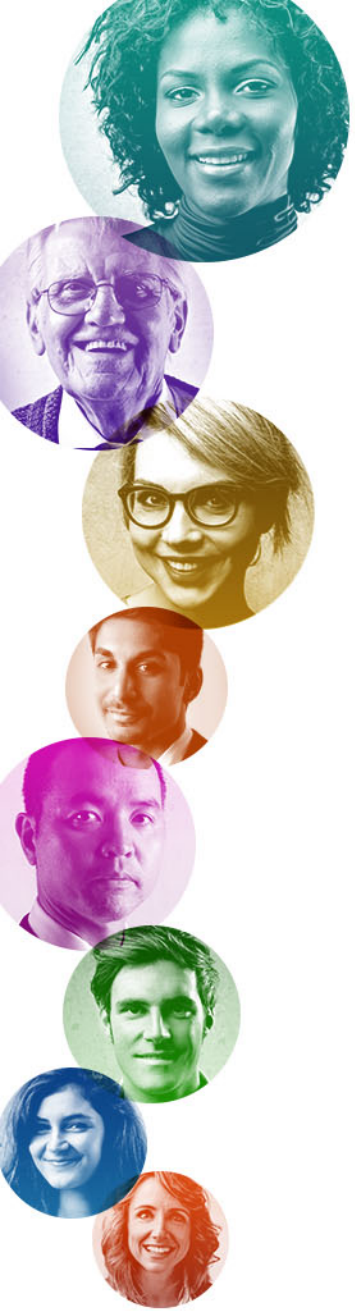
While social media helps us stay more involved, informed, and interconnected than ever before, it comes with risks.

- 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.
- While the Internet is a great place to swap pictures and make weekend plans, 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]

1. Nielsen Media Research, The State of Social Media: The Social Media Report, 2011
2. Johnson & Wales University, The Effects of Social Media on College Students, 2011



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.

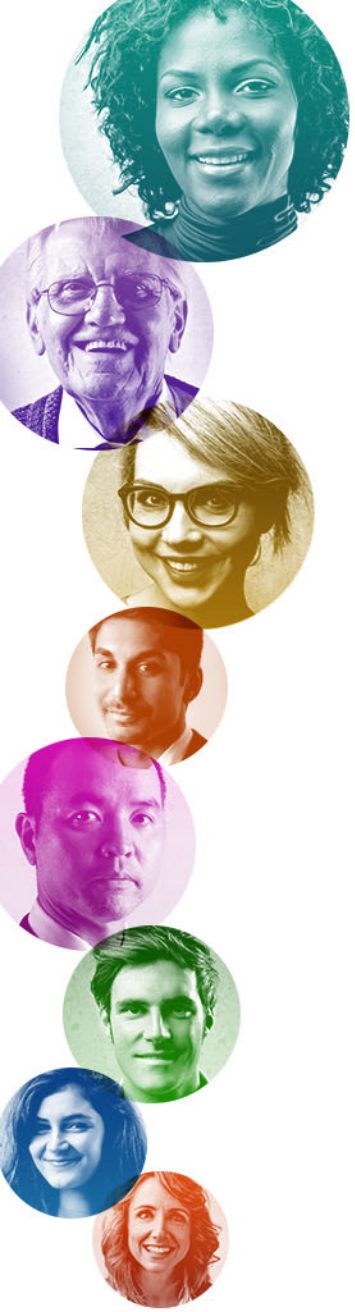
Your social media network has likely expanded to include peers and potential employers who may have access to your photos, comments, check-ins, and status updates. Spend time creating appropriate privacy settings for the various members of your network.

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.

Only 18 percent of young adults claim they are comfortable with what their friends post about them online, and 32 percent say that the information about them online is what they choose for the public to see.[1]

1. Pew Research Center, “Teens, Social Media, and Privacy.” May 2013



CYBER PREDATORS

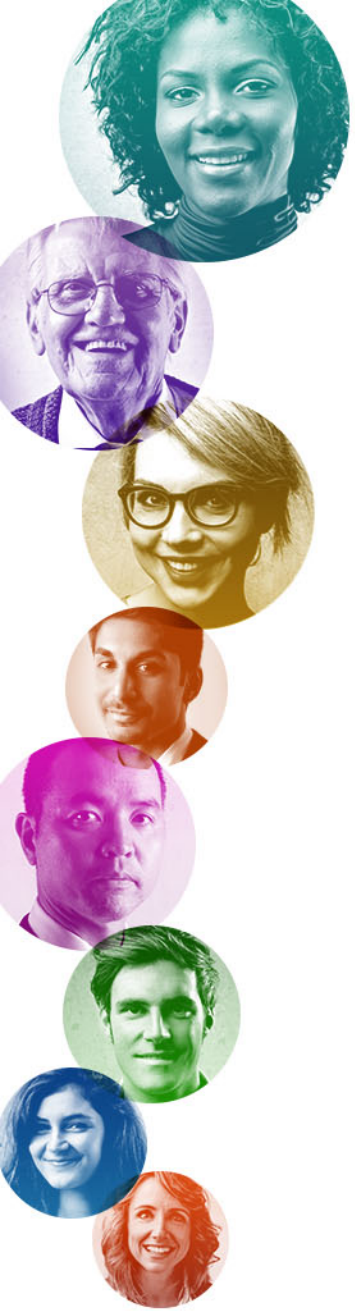
Cyber predators *are people who search online for other people in order to use, control, or harm them in some way.*

Cyber stalking *refers to harassing behavior engaged in repeatedly, such as following a person, appearing at a person's home, or leaving written messages or objects.*

1 in 5
Americans have been affected by cyber stalking

Cyber Tips for Young Adults:

- **Create strong passwords.** Use a mix of letters, numbers and characters (Example: I love to dance! → 1L0v32Danc3!)
- **Clean up your online profiles.** Don't include your address or phone number
- **Lockdown your privacy settings.** Make sure to set all of your privacy settings to "private" or "friends only"
- **Be careful whom you connect with.** When using social networking sites, only connect with people who you know in real life (and not just people with mutual friends either)
- **Avoid using location-based services.** "Checking in" to restaurants and other locations can be fun, but it can also be dangerous if someone is stalking you



IDENTITY THEFT

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

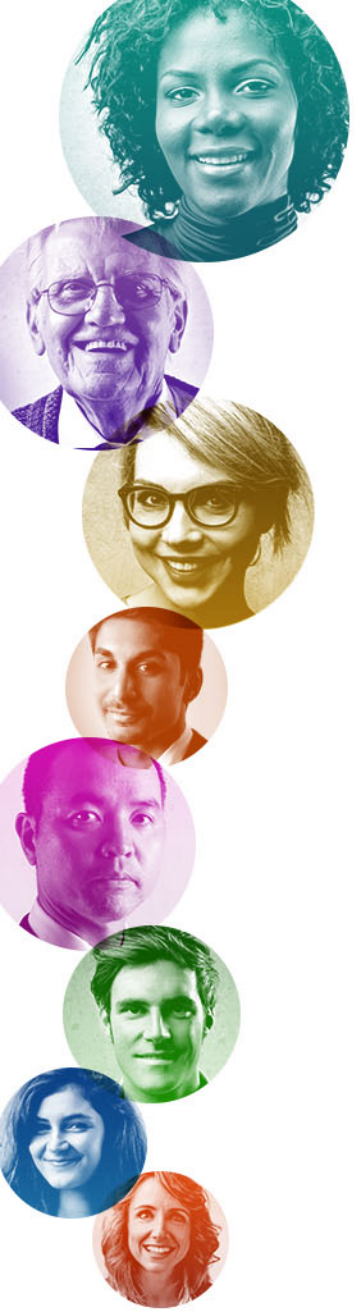
Cyber Tips for Young Adults:

- Create strong passwords with eight characters or more that use a combination of numbers, letters, and symbols (Example: I got a blank space! → 1G0tABlankSpac3!).
- 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

- **18-29 year olds** issue the most identity theft complaints.
- **31%** of all identity theft complaints received by the Federal Trade Commission in 2012 were filed by young adults.[1]

1. Source: Federal Trade Commission, 2012

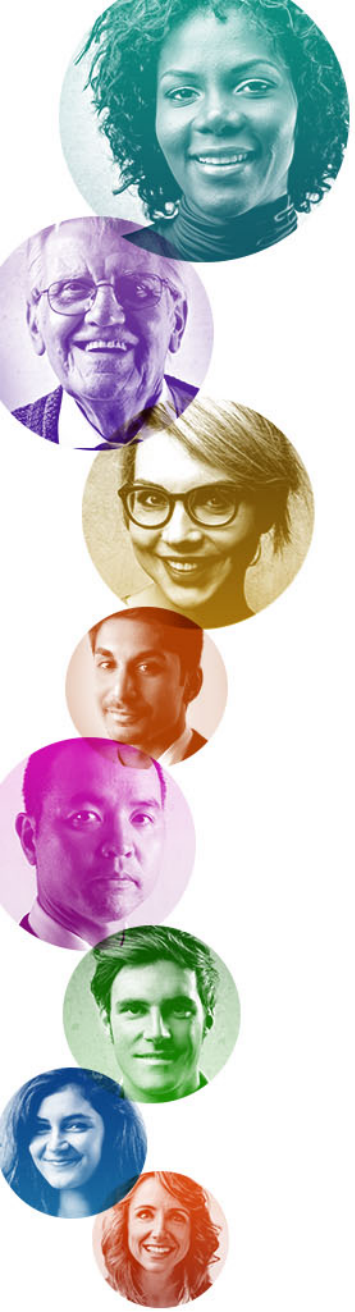


FRAUD & PHISHING

__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 a user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.

Cyber Tips for Young Adults:

- Most organizations – banks, 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.
- 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.
- 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 the link.



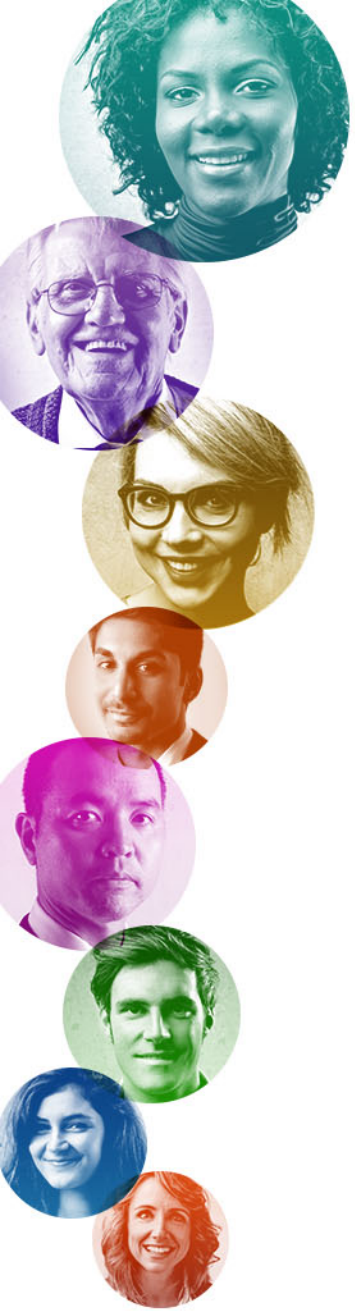
MOBILE SECURITY

A study by Pew Research Center found that almost all Americans (90%) now have a cell phone and 58% own a smartphone.

We are increasingly using phones for banking, online shopping, and social media. The more we travel and access the Internet on the go, the more risks we face on our mobile devices.

Tips for Securing Mobile Devices:

- **Think Before You Connect**. Before you connect to any public Wi-Fi hotspot, confirm the name of the network and exact login procedures to ensure that the network is legitimate.
- **Guard Your Mobile Device**. In order to prevent theft, unauthorized access, and loss of sensitive information, never leave your mobile devices unattended in a public place.
- **Keep It Locked.** Always lock your device when you are not using it. Use strong PINs and passwords to prevent others from accessing your device.
- **Update Your Mobile Software.** Keep your operating system software and apps updated, which will improve your device's ability to defend against malware.
- **Only Connect to the Internet if Needed.** Disconnect your device from the Internet when you aren't using it and make sure your device isn't programmed to automatically connect to Wi-Fi.
- **Know Your Apps**. Be sure to thoroughly review the details and specifications of an application before you download it. Delete any apps that you are not using to increase your security. Double-check how the app will be using your information (Example: does it need access to your pictures or contact list? If so, why?)

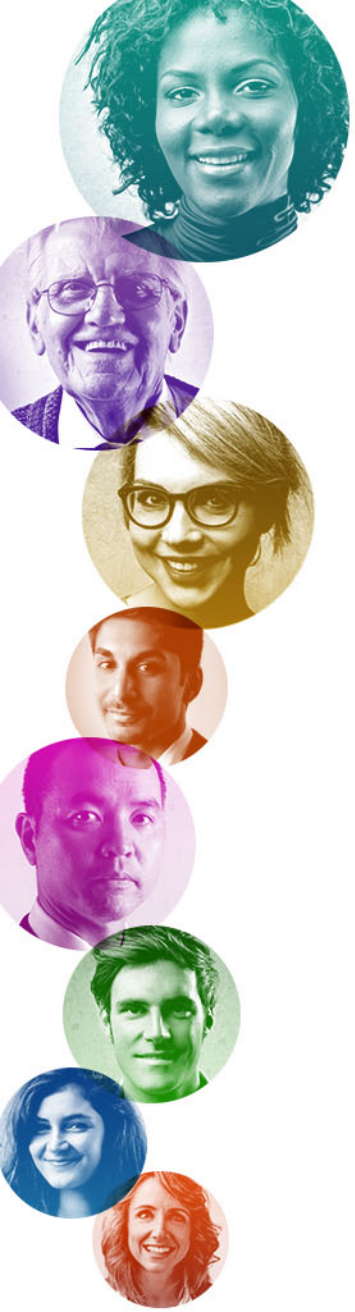


CALL TO ACTION

Cybersecurity is a shared responsibility that all Americans should embrace 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**.
- 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.
- Remind your friends that their online behavior can affect you too so it's important to use technology safely (example: if they download a suspicious app and it takes their information, your contact information or pictures with you in them can also be taken).
- Volunteer within your community to mentor kids and teens on the basics of online safety.

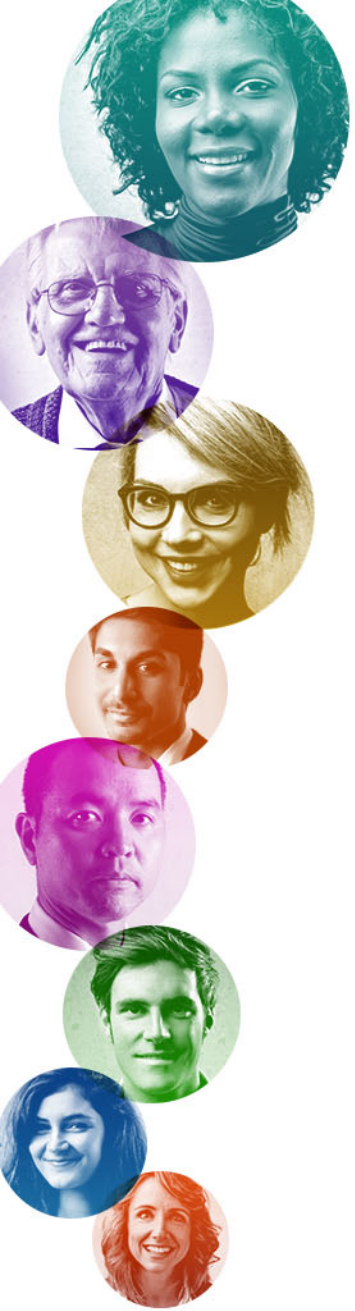


CYBER EDUCATION

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.**
- Find out what programs, classes, and scholarships are available to you at your college or university.

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/**.



LEARN MORE

- 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.


YOU CAN HELP KEEP
THE INTERNET SAFE
Homeland Security
STOP | THINK | CONNECT