Stop.Think.Connect.

NICE Workshop Stop.Think.Connect. Session
September 17, 2013

Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) Division
Office of Cybersecurity and Communications (CS&C)
U.S. Department of Homeland Security (DHS)

Homeland Security

Stop.Think.Connect. Campaign

In 2009, President Obama issued the **Cyberspace Policy Review**, which tasked DHS with creating an ongoing cybersecurity awareness campaign to educate and empower Americans to be safer and more secure online.

Stop.Think.Connect.™ is part of an unprecedented effort among federal and state governments, industry, and non-profit organizations to promote safe online behavior and practices.

DHS provides the federal government's leadership for Stop.Think.Connect., a message originally developed by the Anti-Phishing Working Group and National Cyber Security Alliance (NCSA).

The Campaign launched in October 2010 in conjunction with National Cybersecurity Awareness Month (NCSAM).

Partnership Model

The Stop.Think.Connect. Campaign relies on partner organizations to amplify the message among various audiences.

Through its **Cyber Awareness Coalition**, the Campaign works with government partners including federal agencies and state, local, territorial, and tribal (SLTT) governments.

The Stop.Think.Connect. **National Network** is a consortium of non-profit groups that advocate and promote cybersecurity within their organizations and to their stakeholders.

DHS engages with industry through its partnership with NCSA.

As of September 2013, the Coalition has expanded to 35 government members and the National Network has expanded to 34 organizations.

Grassroots Outreach

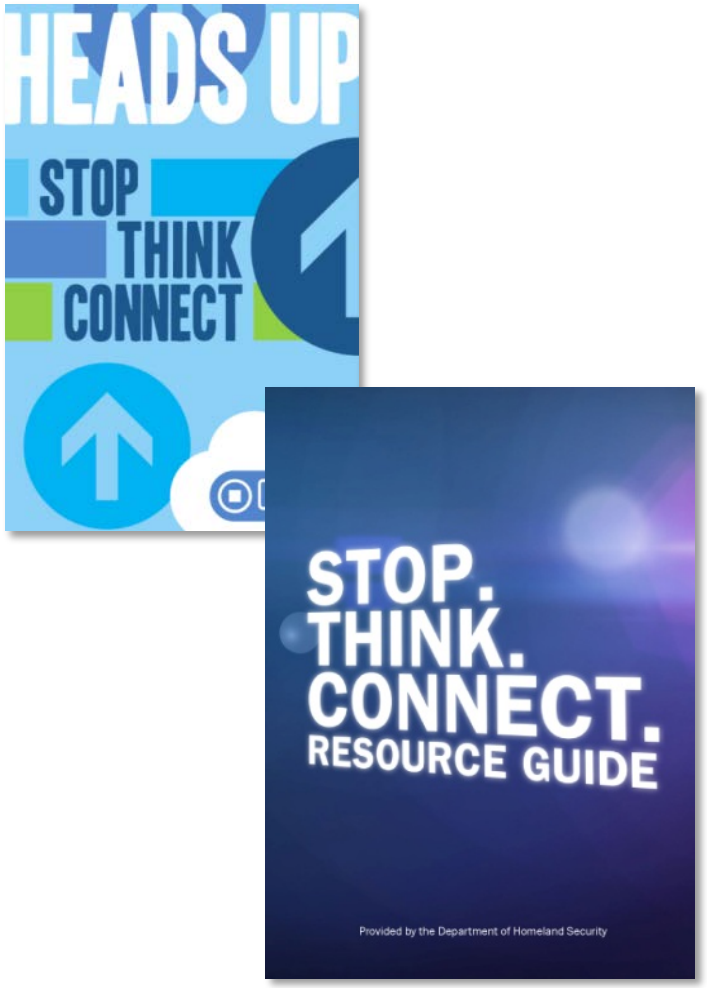
DHS encourages individuals to share the Stop.Think.Connect. Message, underscoring that cybersecurity is a shared responsibility.

The ***Friends* of the Campaign** program is a grassroots outreach effort for individuals to sign-up and commit to become messengers of the Stop.Think.Connect. Campaign.

The DHS shares a monthly newsletter that highlights resources, partner efforts, and actionable tips for individuals.

More than 33,000 people have signed up to become *Friends* and receive information from the Campaign.

Resource Distribution



DHS provides a number of resources to the public.

The **Stop.Think.Connect. Toolkit** provides materials designed for:

- Students (K-8, 9-12, and undergraduate)
- Parents and Teachers
- Young Professionals
- Older Americans
- Government
- Industry
- Law Enforcement

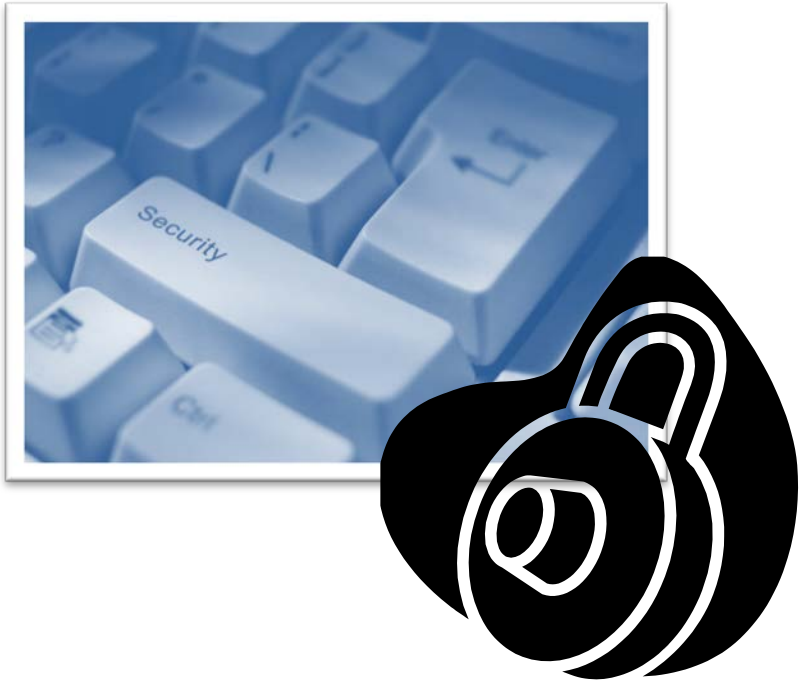
Materials are available online at:

www.dhs.gov/stopthinkconnect

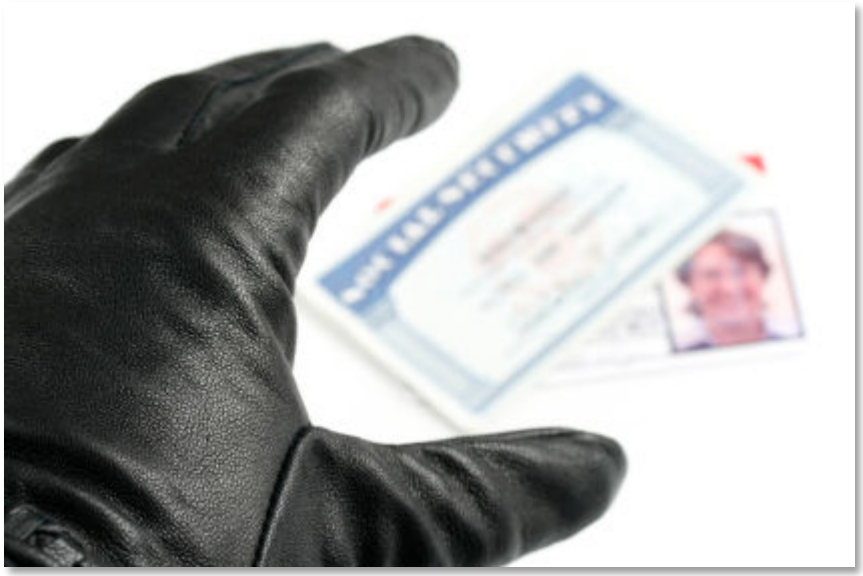
Audiences and Cyber Trends

The Campaign provides tips and resources to address various cyber trends for differing demographics including:

- Identity Theft
- Fraud & Fishing
- Your Online Identity



Identity Theft



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 something to you and you only
- Lock your computer and cell phone
- Only open emails from people you know and don’t click on links for unfamiliar sites
- Notify law enforcement if you think you’ve been a victim of identity theft at the FBI’s Internet crimes complaint center: www.ic3.gov

Did You Know?

- **Credit card data theft has increased 50% from 2005 to 2010[1]**
- **18% of 2 million complaints to the FTC are related to identity theft[2]**

1. USA Today – Identity theft growing, costly to victims, April 14, 2013. J. Craig Anderson
2. FTC: Identity theft retains its throne as No.1 worst scourge in Top 10 consumer complaint list. Michael Cooney, Network World February 26, 2013

Fraud & Phishing

Fraud is the intentional perversion of truth in order to induce another to part with something of value.

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?

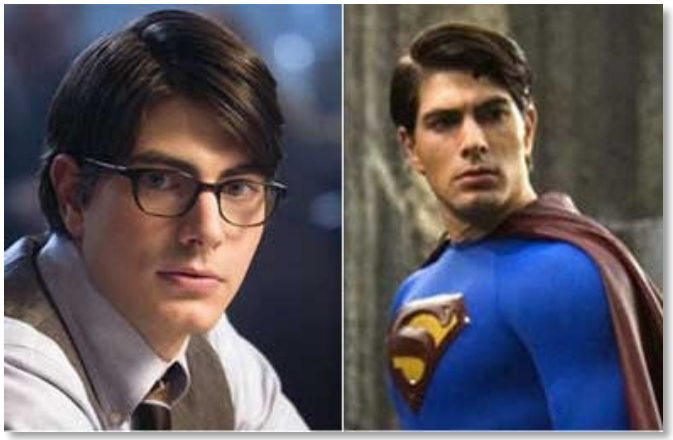
- **25% of Internet users have had their computer infected by a virus, most likely from an email message[1]**
- **26% of Internet users have reported that their personally identifiable information was compromised because of a data break in the last year[2]**

1. Pew Internet: Internet Crime
2. NCSA

Tips

- Beware of requests to update or confirm your personal information. Most established organizations don't ask for information via email
- Don't open emails from strangers and don't click on unfamiliar sites; if an offer is too good to be true, then it probably is
- Change your passwords often and avoid using the same password on multiple sites
- Report phishing scams to the Anti-Phishing Work Group at www.apwg.com

Your Online Identity



Did You Know?

- **Only 44% of adults ages 18-29 limit the amount of personal information they share online[1]**
- **Of social media users, only 42% have changed their passwords to maintain security[2]**

Your online identity can only be managed by you. As your information becomes increasingly available to others, make sure you are taking steps to protect yourself.

Tips

- Set up privacy restrictions**.** Set up the appropriate settings for the members of your network - that may include peers and managers - who might have access to your photos, comments, check-ins, and status updates
- Think about your future. Do a quick search of yourself and consider setting up alerts for searches on different variations of your name with your school, place of employment, and other distinguishing details

1. Pew Internet 2010
2. NCSA/McAfee Online Study 2012

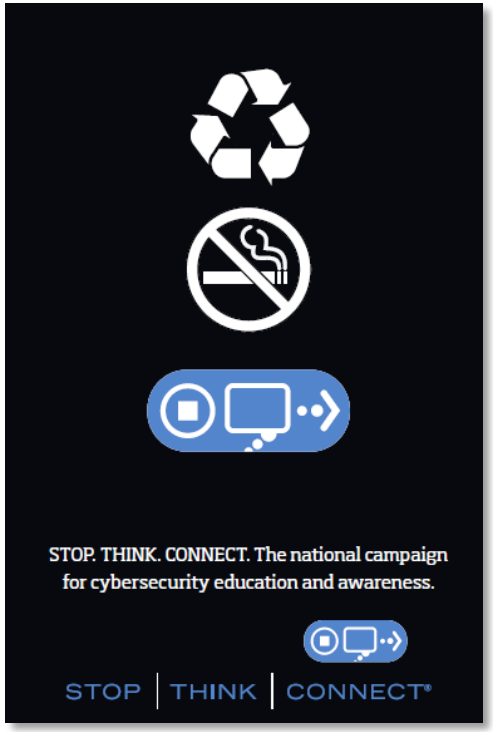
Call to Action

Cybersecurity is a shared responsibility that everyone must adopt in order to keep the global online community secure in the 21st Century.

We invite you to join us to educate and empower online citizens to take steps to protect themselves and their families online.

How to get involved:

- Sign up to become a *Friend* of the Campaign
- Formally adopt the Stop.Think.Connect. messaging and share materials and resources with your organization
- Promote and distribute Campaign resources to schools, businesses, and community organizations
- Get involved and participate in NCSAM 2013



National Cyber Security Awareness Month

October is **National Cyber Security Awareness Month (NCSAM)**. NCSAM engages public and private sector partners around the country to raise awareness and educate Americans about cybersecurity. NCSAM is sponsored by DHS, NCSA, and the Multi-State Information Sharing and Analysis Center (MS-ISAC).

Celebrating it's 10th year, NCSAM has been formally recognized by the President; Congress; federal, state and local governments; and leaders from industry and academia.

In 2012, NCSAM was coordinated with international partners from Canada and the European Union for the first time.

NCSAM is the culmination of yearlong Stop.Think.Connect. Campaign efforts, highlighting cyber awareness successes.

NCSAM 2013

Each week in October is dedicated to a specific cybersecurity theme. The themes offer an opportunity for government and industry to get involved in the cybersecurity activities most relevant to them. To engage Americans across the nation, key events are coordinated in geographically diverse locations.

- ***Week 1, October 1-4, 2013*** *– Our Shared Responsibility; Stop.Think.Connect., and Cybersecurity in the Next 10 Years, Boston, MA*
- ***Week 2, October 8-11, 2013*** *– Being Mobile: Online Safety and Security, Washington D.C.*
- ***Week 3, October 15-18, 2013*** *– Cyber Workforce and the Next Generation of Cyber Leaders, Los Angeles, CA*
- ***Week 4, October 21-25, 2013*** *– Cyber Crime, Chicago, IL/New York, NY*
- ***Week 5, October 28-31, 2013*** *–, Critical Infrastructure and Cybersecurity, Washington D.C.*

10TH ANNIVERSARY
National Cyber Security Awareness Month

Contact Us

For additional information, please contact:

Stopthinkconnect@dhs.gov

Or visit:

www.dhs.gov/stopthinkconnect

For additional information about National Cyber Security Awareness Month, visit:

www.dhs.gov/national-cyber-security-awareness-month