• 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.

• The Stop.Think.Connect. Campaign launched on October 4, 2010, in conjunction with National Cyber Security Awareness Month.

• 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.
CAMPAIGN’S GOALS AND OBJECTIVES

*Raise awareness among Americans about cybersecurity, empower them to be safe online and educate the next generation of the cyber workforce.*

**OBJECTIVES**

1. Increase and reinforce awareness of cybersecurity.

2. Work with national organizations in educating the public about cybersecurity.

3. Engage the American public to acknowledge and commit to the **shared responsibility** of securing cyberspace.

4. Promote science, technology, engineering, and math (STEM) education to build the cyber workforce.
POLL THE AUDIENCE:

Do your children know more about the Internet and technology than you do?

What is cybersecurity?

Do your kids have their own computers? Do they have their own cell phones?

Do you set rules for Internet use? If so, what are they?

What are your main concerns about kids using the Internet?
KIDS LEAD DIGITAL LIVES

- On average, kids 10 and older spend approximately 6 hours a day online.

- Most parents estimate their child spends 4 hours a day online, which is wrong.

- Most kids access to the Internet becomes more mobile—cellphones, tablets, etc.—as they age.

Source: McAfee Digital Deception Study 2013
Seventy-four percent of parents admit to not knowing about their children’s online behavior, but 46% of youth say that they would change their online behavior if their parents were paying attention.¹

- Create an open and honest environment for discussing online behaviors and security risks with kids.
- Start conversations regularly about practicing online safety and focus on offering guidance instead of trying to control children’s online behavior.
- Emphasize the concept of credibility and encourage children to proceed with caution: not everything they see on the Internet is true and people on the Internet may not be who they appear to be. Talk with children, and especially teens, about the importance of creating and maintaining a positive online identity.
- Watch for changes in behavior—if your child suddenly avoids the computer—it may be a sign they are being bullied online.
- Review security settings and privacy policies for the websites your child uses.

¹ McAfee Digital Deception Study 2013
Cyber ethics help Internet users understand what type of online behavior is right and wrong. Cyber predators are people who search online for other people in order to use, control, or harm them in some way. Cyberbullying is the electronic posting of mean-spirited messages about a person, often anonymously.

DID YOU KNOW?

• Over 50% of sexual exploitation victims are between the ages of 12 and 15.¹
• Seven in 10 young people are victims of cyberbullying and 37% experience cyberbullying on a frequent basis.²

TIPS

• Keep 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 is in cyberspace, it is out there forever.
• Stop any questionable online behavior; only do and say things online that you would do in real life.
• Speak up. If you see something inappropriate, let the website know and tell an adult you trust. Don’t stand for bullying—online or off.

² Ditch the Label Annual Cyberbullying Survey 2013
**Identity Theft**

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

**DID YOU KNOW?**

- In 2012, children ages 19 and under made up 6% of all identity theft cases.¹
- 56% of cases reporting misuse of a social security number are for children.²

**TIPS**

- Don’t use the same password on multiple websites.
- Choose a password that means something to you and you only.
- Lock your computer and cell phone when they are not in use.
- Don’t share personal information without knowing exactly who is on the receiving end. Use strong passwords with eight characters or more and a combination of letters, numbers and symbols; don’t share them with anyone other than your parents.
- Don’t open emails from strangers and avoid clicking on links for unfamiliar sites; if you think an offer is too good to be true, then it probably is.

---

¹ Federal Trade Commission, 2012
² 2012 Child Identity Fraud Report
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.

**DID YOU KNOW?**
- A study shows that 30% of teens have admitted to meeting someone online who claimed to be someone they were not, using fake photos and fake identities.¹
- In 2012, 1 in 40 reported cases of identity theft were for adolescents ages 18 and below.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 avoid clicking on links for 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 web addresses by hand instead of following links.

---

¹ Raytheon, commissioned by NCSA, “Preparing Millennials to Lead in Cyberspace”, 2013
² ITAC, 2012 Child Identity Fraud Report
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/.
RESOURCES AVAILABLE TO YOUR FAMILY

**OnGuardOnline.gov**: This website, run by the Federal Trade Commission, is a one-stop shop for online safety resources available to parents, educators and kids.

**CyberTipline.com**: The Congressionally mandated CyberTipline, which is part of the National Center for Missing and Exploited Children (NCMEC), receives online child solicitation reports 24-hours a day, seven days a week. Submit an online report or call 1-800-843-5678.

**StaySafeOnline.org**: The National Cyber Security Alliance offers information on security updates, free antivirus software, malware software removal, and other services.
CALL TO ACTION

Cybersecurity is a shared responsibility that all Americans must adopt in their communities to keep the nation secure in the 21st Century. **Become an advocate in your community** to help educate and empower the public to take steps to protect themselves and their families online.

**HOW TO GET INVOLVED:**

- Download and distribute Stop.Think.Connect. materials, such as the brochure, bookmark and poster, in your neighborhoods and communities.
- Lead or host a cyber awareness activity in your place of work, school, recreation, or worship.
- Discuss the importance of cybersecurity with your friends and family.
- Inform your community about the Stop.Think.Connect. Campaign and the resources available.
- Blog or post about the issue of cybersecurity and the Stop.Think.Connect. Campaign.
- Get schools and community organizations involved and informed on cybersecurity.
SECURING CYBERSPACE STARTS WITH YOU