



INTERNATIONAL CYBER AWARENESS PROGRAMS NEW CAMPAIGN PACKET

Welcome to the Department of Homeland Security (DHS) Stop.Think.Connect.™ Campaign packet for new international cyber awareness programs. The following document lays out necessary steps and best practices for starting up a new cybersecurity awareness campaign in a country that does not currently run the Stop.Think.Connect. Campaign.

The new campaign packet contains three major sections:

- **Section 1: Cybersecurity Awareness Campaign Best Practices Checklist** lays out the relevant steps to begin an awareness campaign and develop both materials and relationships to spread messaging.
- **Section 2: Cybersecurity Awareness Campaign Sample Communications Plan** builds on the best practices checklist by providing a template communications plan that describes each section of a successful communications plan, followed by examples from the DHS Stop.Think.Connect. communications plan.
- **Section 3: Cybersecurity Awareness Campaign Metrics** describes the type of metrics the Stop.Think.Connect. Campaign uses to track and evaluate its cyber awareness programming, which may serve as a useful baseline for new campaigns establishing their own measures of effectiveness.

We welcome your input and suggestions. If you have any questions or comments, feel free to email stophinkconnect@dhs.gov.



SECTION 1: CYBERSECURITY AWARENESS CAMPAIGN BEST PRACTICES CHECKLIST

Purpose

This section outlines best practices for incorporating the Stop.Think.Connect.™ Campaign into new countries. The best practices are modeled after the U.S. version of the Stop.Think.Connect. Campaign, a nationwide cybersecurity awareness effort that aims to help people understand cyber threats and how to protect themselves online.

While every country has unique needs and challenges related to cybersecurity threats and protection, the following best practices can help when launching a version of the Stop.Think.Connect. Campaign. A checklist shows the basic steps, followed by explanations that are more detailed:

- Make a plan (see **Section 2: Cybersecurity Awareness Campaign Sample Communications Plan** for more information)
- Create and/or tailor educational resources
- Use social media
- Partner with organizations
- Connect with individuals
- Measure effectiveness (see **Section 3: Cybersecurity Awareness Campaign Metrics** for sample metrics)

Best Practices

1. **Develop a strategic plan, including well-defined goals and objectives and primary target audience(s).** The first step to incorporating Stop.Think.Connect. is determining specific goals and objectives for the Campaign. From there, create steps to implement the strategy and reach target audiences. To ensure that messaging is appropriately tailored for target audiences, the Stop.Think.Connect. Campaign identified at the outset seven audience groups: students; parents and educators; young professionals; older Americans; government; industry; and small business. Each audience group has unique strengths and needs. The strategic plan should account for the identified audience group's existing cyber knowledge as well as the primary threats it faces.
 - a. *Key messaging should include the Stop.Think.Connect. theme:*
 - **Stop:** Before you use the Internet, take time to understand the risks and learn how to spot potential problems.



- **Think:** Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.
- **Connect:** Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.
- **Stop. Think. Connect.** Protect yourself and help keep the web a safer place for everyone.

b. *Key messaging should also include global best practices.* While messaging should be tailored to a country's needs, certain tips like using strong passwords, keeping operating systems and security software up-to-date, connecting only with people you trust, and avoiding sites that sound too good to be true, can be universally applied.

- 2. Develop targeted communications strategies and resources to reach specific audiences.** Everyone has different cybersecurity needs. For example, students may need to know about cyber predators while IT professionals need to know about hackers. Different materials should be developed for each audience's needs, knowledge, and ability level. The Stop.Think.Connect. Campaign offers tip sheets for each specific audience group to address its unique needs and threats while ensuring the content is at an appropriate level. Comprehensive educational materials, such as the Stop.Think.Connect. [Toolkit](#), emphasize the shared responsibility for cybersecurity while helping ensure that resources are available for all segments of the community. Simple reminders in the form of posters, wristbands, etc. help individuals keep cybersecurity best practices as a top priority. Stop.Think.Connect. Campaign materials can and have been translated and used around the world.
- 3. Use social media.** Much of cybersecurity awareness takes place online. Using social media helps connect cybersecurity awareness messaging to individuals through the channels they are already using—and in some cases, the ones they prefer to use. Posting information on social networking sites like Facebook, Twitter, and YouTube provides a means of engaging and sharing information while also receiving valuable input. The Stop.Think.Connect. Campaign, for example, connects with users in a variety of ways online, including Twitter chats and blog posts that raise awareness on specific topics. You can see examples by viewing the [@Cyber](#) Twitter handle, the DHS [Blog @ Homeland Security](#), and the DHS [Facebook page](#).



- 4. Create and maintain partnerships with allies in target audiences.** No organization, whether government agency, corporation, or non-profit, can single-handedly spread awareness. Both public and private partnerships are essential. Develop and engage partnerships with organizations such as:
- a. *Government agencies.* Government agencies lend authority to the message, and have a wide reach to individuals and communities. The Stop.Think.Connect. Campaign developed the Cyber Awareness Coalition to engage with federal agencies as well as state, local, tribal, and territorial government entities to help them educate their employees and constituents to identify and deter online dangers. Key government partners at various levels include Computer Emergency Readiness Teams (CERTs), Offices of the Chief Information Security Officers (CISOs), and Office of the Chief Information Officers (CIOs).
 - b. *Non-profit organizations.* Non-profit organizations offer a variety of resources and flexibility to spread cybersecurity awareness messaging. The Stop.Think.Connect. Campaign developed its National Network of non-profits to advocate and promote cybersecurity within their organizations and to their members and audiences. Non-profit partners span all audience groups identified in the strategic plan. Regular calls including all partner organizations help build networks between each organization, both public and private.
 - c. *Academic institutions.* Engaging with academic leaders, such as the United States' Department of Homeland Security and National Security Agency-designated Centers of Academic Excellence, ensures that up-to-date research informs awareness programming. It also helps develop relationships between the workforce-in-training and the organizations that will employ them. Developing high school and elementary school partnerships builds a stronger foundation for responsible cyber behavior. Encouraging cybersecurity awareness education from a young age helps students use the Internet safely throughout their lives.
 - d. *Private sector organizations.* Industry leaders, including information, retail, finance, and educational services, can educate employees, consumers, and other audiences about the threats affecting them as well as receive input on strengthening cybersecurity practices. Innovative cybersecurity solutions developed by private sector organizations can drive best practices in both the public and private sectors. DHS' co-leader in the Stop.Think.Connect. Campaign, the National Cyber Security Alliance, coordinates the private sector portion of the Campaign.



5. Engage audiences on the individual level through grassroots efforts.

Individual awareness is foundational to an effective cybersecurity awareness program. The Stop.Think.Connect. Campaign, for example, invites individuals to become *Friends* of the Campaign by signing up for monthly email newsletters with the latest cyber tips, news, and information relevant to them. The Campaign also reaches individuals by conducting outreach events tailored to each audience and providing speakers who can discuss the cybersecurity issues that most affect the audience.

6. Measure whether the effort is truly raising awareness among the target audiences.

To do this, collect feedback from focus groups, surveys, or other tactics. Also, track which webpages are most viewed, which materials are most downloaded, which events are best received, and which practices audiences find most effective to identify successes and foster improvement. Feedback from partner organizations helps future planning focus on effectiveness and creativity.



Additional Startup Resources

For more information and examples of use, please visit the following websites:

- Stop.Think.Connect. Campaign:
 - <http://www.dhs.gov/stopthinkconnect>
 - <http://stopthinkconnect.org/> (National Cyber Security Alliance)
- Communications Strategies and Resources:
 - <http://www.dhs.gov/stopthinkconnect-get-informed>
 - <http://stopthinkconnect.org/resources/> (NCSA)
 - <http://stopthinkconnect.org/tips-and-advice/> (NCSA)
- Social Media:
 - <https://twitter.com/cyber>
 - <http://blog.dhs.gov/>
 - <https://www.facebook.com/homelandsecurity>
 - <https://twitter.com/STOPTHINKCONNECT> (NCSA)
 - <https://www.facebook.com/STOPTHINKCONNECT> (NCSA)
- Partnerships with Organizations:
 - <http://www.dhs.gov/stopthinkconnect-national-network>
 - <http://www.dhs.gov/stopthinkconnect-cyber-awareness-coalition>
- Connecting with Individuals:
 - <http://www.dhs.gov/stopthinkconnect-Friends-campaign-program>
 - <http://www.dhs.gov/stopthinkconnect-your-community>
 - <http://www.dhs.gov/stopthinkconnect-campaign-news>
- Measuring Effectiveness:
 - <http://stopthinkconnect.org/research-surveys/research-findings/> (NCSA)



SECTION 2: CYBERSECURITY AWARENESS CAMPAIGN SAMPLE COMMUNICATIONS PLAN

Purpose

This section provides a sample framework for establishing a communications plan for the Stop.Think.Connect.™ Campaign in other countries. The framework uses the model of the U.S. version of the Stop.Think.Connect. Campaign (otherwise referred to as “the Campaign”), a national effort to help people understand cyber threats and how to protect themselves online.

While every country has unique needs and challenges when communicating to their citizens, the following sample plan can help a country launch its own version of the Campaign. Each section of the plan briefly describes the type of content that should go in that section, followed by an example from the U.S. plan. The primary sections of any communications plan include:

- Purpose and Background
- Overarching Communications Goals
- Communications Objectives
- Key Target Audiences
- Communications Channels
- Strategies
- Messaging
- Roles and Responsibilities
- Resources
- Challenges to Communication
- Measurements of Success/Metrics

Sample: Purpose and Background

The Purpose lays out why to write a communications plan and what the plan aims to accomplish. Optionally, it may include a brief Background on the Campaign for context.

The preceding section is an example of the Purpose and Background.



Sample: Overarching Communications Goals

Overarching communications goals are high-level aims for the cybersecurity awareness program. Such goals are strategically broad while remaining measurable. For example, the U.S. Department of Homeland Security's (DHS) overarching communications goal for the Campaign follows:

The overarching goal of the Campaign is to promote public awareness about cybersecurity by increasing the level of understanding of cyber threats, simple mitigation actions, and empowering the American public to be more prepared online to:

- Elevate the Nation's awareness of cybersecurity and its association with the security of our Nation and safety of our personal lives
- Engage the American public and the private sector as well as state and local governments in our Nation's effort to improve cybersecurity
- Generate and communicate approaches and strategies for Americans to keep themselves, their families, and communities safer online

Sample: Communications Objectives

Communications objectives are more specific than goals, describing how to achieve the strategies outlined in the goals. Like overarching goals, the objectives should be measurable. DHS communications objectives for the Campaign are to:

- Educate the American public on cyber safety practices to protect themselves and ensure stakeholder groups are aware of available resources (from DHS and others)
- Increase the number of national stakeholder groups engaged with the Campaign and strengthen existing relationships with State and local governments, industry, non-profits, school systems, and educators
- Increase and strengthen the cyber workforce by promoting science, technology, engineering, and math (STEM) education

Sample: Key Target Audiences

Identifying key audiences helps ensure that messaging focuses on those most receptive to or in need of the message. Clearly defining those audiences keeps the messaging targeted to specific groups by maintaining a shared understanding of what audience titles mean.

The Campaign identified at the outset seven audience groups: students; parents and educators; young professionals; older Americans; government; industry; and small business. As an example of audience group definitions, the Campaign considers older Americans to be individuals who are 60 years of age and older, as defined by the Office of Aging, Department of Health and Human Services.



Sample: Communications Channels

Communications channels include all the ways to convey messaging to the audience. Carefully consider all currently used means of communication, as well as additional methods available for use. Although the following examples are brief synopses, the communications plan should clearly specify both what the channels are and how to use them.

The Campaign engages audiences through the following channels:

- Events: Hosting events with target audience groups
- Traditional Media: Proactively reaching out to national/regional/local media (e.g., broadcast, print, web)
- Social Media: Actively using social media platforms (DHS blog, Facebook, Twitter)
- Newsletter: Distributing a monthly newsletter as well as informational toolkits
- Website: Regularly updating campaign websites with news, tips, and key information
- Partners: Encouraging outreach from partner organizations

Sample: Strategies

Campaign strategies take into account both the practical methods of disseminating information and the ways of creating campaign momentum and growth. Each broad strategy contains many small steps to accomplish it, and both the steps and the strategies should be flexible enough to adapt to a changing environment. The example below includes only a few strategy samples of the U.S. Stop.Think.Connect. Campaign.

The Campaign uses the following strategies, among others, to meet its communication objectives:

1. Disseminate Campaign messaging through events and media (social and traditional)
2. Build a cadre of messengers via partnerships with non-profits and grassroots outreach
3. Work across the Federal interagency to collaborate on events and messaging



Sample: Messaging

Topline messaging focuses on the core messages that every Campaign outreach incorporates. At a minimum, this includes the following Stop.Think.Connect. themes:

- **Stop:** Before you use the Internet, take time to understand the risks and learn how to spot potential problems
- **Think:** Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's
- **Connect:** Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer
- **Stop. Think. Connect.** Protect yourself and help keep the web a safer place for everyone

Other universally applicable messages include using strong passwords, keeping operating systems and security software up-to-date, connecting only with people you trust, and avoiding sites that sound too good to be true.

Each country and campaign—and each audience and event—has specific needs that require tailored messaging. Topline messaging serves as the foundation for each of those customized outreaches.

Sample: Roles and Responsibilities

Clearly designating roles and responsibilities enables teams to work together effectively while preventing overlap or confusion. Such differentiation occurs between organizations when multiple groups support a campaign, as well as among team members of a particular organization. For example, as part of the overarching Stop.Think.Connect. Campaign, DHS coordinates relationships with non-profit organizations and government agencies while its partner, the National Cyber Security Alliance (NCSA), coordinates with industry.

Sample: Resources

Listing the resources available to a Campaign makes clear the scope and limitations for outreach activities within a given time period. For example, it may include specified staff, time, materials, and products. The Campaign currently has a toolkit that is comprised of posters, tip cards, bookmarks, and other helpful resources for each of its audience groups.



Sample: Challenges to Communications

Recognizing the challenges to communications helps overcome gaps and obstacles. Examples for the Campaign include the following:

- Technical aspects of cyber threats are difficult for audiences to comprehend and understand how it relates to them
- The general public does not necessarily see cyber threats as real or pertinent to their everyday lives

Sample: Measurements of Success/Metrics

Any communications plan needs a way to receive feedback and measure effectiveness. Due to the nature of the Campaign, such measurements typically focus on outward activities more than input, but timely feedback is essential.

Examples of Campaign metrics include:

- Number of participants for each event or series of events in a region
- Number of collateral distributed
- Fair and balanced media coverage
- Number of stakeholders involved (e.g., *Friends*, Cyber Awareness Coalition members, National Network members, etc.)
- Hits to webpage
- Feedback and testimonials from participants and partner organizations
- Feedback from Congress, state and local leaders/officials



SECTION 3: CYBERSECURITY AWARENESS CAMPAIGN METRICS

Purpose


This section describes the type of metrics the U.S. Department of Homeland Security's (DHS) Stop.Think.Connect.™ Campaign uses to track and evaluate its cyber awareness programming.¹ As the international community adopts the Campaign, countries may find the outlined metrics useful as a baseline for establishing their own measures of effectiveness.

The metrics fall into several broad categories; how these types of categories are applied to differing cybersecurity awareness programs depends on particular programs' goals and resources. **Stakeholder Engagement** deals with formal partnerships with government agencies and non-profit organizations. **Traditional Media Outreach** and **Digital and Online Outreach** each apply to distributing written and multimedia products through established communication channels. **Events and Forums** and **Resources** each cover in-person interactions. A combination of metrics categories is required to understand and measure the full scope of the Campaign.

Metrics Categories and Examples

- **Stakeholder Engagement.** The Campaign partners with a number of non-profit organizations that form its National Network, as well as with federal, state, local, tribal, and territorial government agencies that compose its Cyber Awareness Coalition. The Campaign measures the number of organizations in each of these stakeholder groups, as well as growth rates per year and the number of people reached by each partner organization.
 - By December 2013, **the National Network grew to 36 organizations, including the Boys & Girls Clubs of America, YWCA, National Sheriffs' Association, and Neighborhood Watch.** Through these and other organizations the Campaign reaches Americans nationwide, including parents, educators, students, small businesses, older Americans, and young professionals. With the help of the Campaign, National Network members have instituted many successful cyber awareness efforts, such as providing cyber awareness training for more than 1,500 D.A.R.E. officers. In 2013, the National Network grew by 64%.
 - By December 2013, **the Cyber Awareness Coalition grew to 50 government partners, ranging from the Department of Education to the State of California,** that promote awareness about cyber threats and online safety practices within their organizations and to their constituents. The Campaign has worked with its Coalition members to help spread cybersecurity messaging and combat threats. For example, the Federal

¹ This document is updated annually. Figures are current as of December 2013.



Communications Commission worked with the Campaign, and other agencies, on the development of its Smartphone Security Checker and Small Biz Cyber Planner. Also, the Campaign and the Federal Trade Commission partner on digital outreach and created co-branded community outreach toolkits that have been distributed nationwide to help educate Americans on protecting themselves online. In 2013, the Cyber Awareness Coalition grew by 85%.

- **Traditional Media Outreach.** The Campaign encourages awareness through a number of traditional media sources. Metrics track the number of print circulation hits; online impressions; broadcast reach; articles online and in print; television, radio, and audio news releases; and independent press releases.
- **Digital and Online Outreach.** Many of the Campaign’s resources are distributed online, allowing for ample opportunity to measure interaction and feedback. The Campaign measures the number of: *Friends of the Campaign*; hits to the DHS Stop.Think.Connect. Campaign website; Twitter chats and Facebook Events; Tweet mentions; Facebook “Likes;” and number of blog entries posted.
 - **Friends of the Campaign:** The Campaign reaches people in their own communities through its *Friends of the Campaign* effort. The *Friends* program is a grassroots outreach effort that enables individuals to sign up and commit to becoming messengers of the Stop.Think.Connect. Campaign. An average of **720 people joined the Friends of the Campaign** each month in 2013. The Campaign distributes **monthly newsletters with tips and information about safer online practices to Friends of the Campaign.**
 - **Stop.Think.Connect. Campaign Website:** Campaign materials point users to the website www.dhs.gov/stopthinkconnect. The Campaign tracks the total number of visits to the site as well as which pages and materials are most accessed. There were over 50,580 hits to the website in 2013.
 - **Social Media:** The Campaign participates in regular Twitter chats through [@Cyber](https://twitter.com/Cyber) and posts blogs on the [Blog@Homeland Security](http://Blog@HomelandSecurity). The Campaign measures the number of blog posts and Twitter chats each year, as well as the impressions from the Twitter chats. For example, a series of Twitter chats for National Cyber Security Awareness Month 2013 had an estimated 14,385,000 impressions. Additionally, the Campaign works with the National Cyber Security Alliance (NCSA) to monitor the number of Twitter followers and retweets as well as Facebook *Friends* and “likes” on [@STOPTHINKCONNECT](https://www.facebook.com/STOPTHINKCONNECT) and the Stop.Think.Connect. Facebook accounts.



- **Events and Forums.** The Campaign conducts grassroots events across the Nation to encourage communities to embrace a more sustained, proactive approach to online safety. The location and audience for community events are based upon market analysis that considers statistics on demographics and trends so the Campaign can strategically reach target audiences. For example, as part of National Cyber Security Awareness Month, the Campaign organized a special forum for federal, state, and local law enforcement officials to address electronic-based crimes in South Florida, where identity theft cases are the highest in the Nation. In addition to tracking the number of events, the Campaign analyzes the demographic groups and geographic areas reached by the events.
- **Resources.** The Stop.Think.Connect. [Toolkit](#) provides resources for all ages and segments of the community, including materials to host independent cybersecurity awareness discussions or activities. The Campaign monitors the number of materials distributed, which is typically several thousand per year.