NCSAM Resource Kit

Last reviewed: December 2017

October is National Cyber Security Awareness Month! Some quick links to get you started...

1. First, take a few minutes to complete this 8-question **NCSAM Planning Guide worksheet** (PDF or Word) to help you think about what resources and materials may be required.
2. Visit our toolkits to find sample materials and free, adaptable resources: **Cybersecurity Awareness Resource Library**, **Security Awareness Quick Start Guide**, and **Security Awareness Detailed Instruction Manual**.
3. Find a guest speaker using our **Speakers Bureau**.
4. Learn about the 2017 weekly themes in October and download free materials at **StaySafeOnline.org** or **Stop.Think.Connect.**
5. Keep reading to learn more about **security awareness**, **why security awareness is important**, **critical success factors for awareness activities**, **National Cyber Security Awareness Month**, **how we plan for NCSAM**, and additional **resources** (including links to state, regional, and international efforts).
6. Make plans for a year-round security awareness and education campaign by using our annual **Campus Security Awareness Campaign** materials, whether you promote topics monthly or quarterly. (*2018 guest blogs now available!*)

More than 200 colleges and universities joined EDUCAUSE, Internet2, and the REN-ISAC to show their support as official NCSAM champions in 2017.

CHAMPION
National Cyber Security Awareness Month

Champion registration for 2018 will be available on the National Cyber Security Alliance website in May.

What is Cyber Security Awareness?

The Oxford English Dictionary defines *awareness* as "The quality or state of being aware; consciousness." *Aware* is defined as "Informed; cognizant; conscious; sensible."

The purpose of cyber security awareness presentations is simply to focus attention on cyber security. Awareness presentations are intended to allow individuals to recognize information technology security concerns and respond accordingly.

- The learner is the *recipient* of information
- The information reaches broad audiences
- Attractive packaging techniques are used

We can characterize a user's cyber security awareness level by describing it as the actions a user takes in a given security situation. Do they know about any policies governing that activity? Do they follow the policy? What happens when they are confronted by a new situation that is not addressed by the policy?

Why is Cyber Security Awareness Important?

To protect the confidentiality, integrity, and availability of information in today's highly networked systems environment requires that all individuals:

- Understand their roles and responsibilities related to the organizational mission
- Understand the organization's information technology security policy, procedures, and practices
- Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible

Cyber security awareness programs impress upon users the importance of cyber security and the adverse consequences of its failure. Awareness may reinforce knowledge already gained, but its goal is to produce security behaviors that are automatic. The goal is to make "thinking security" a natural reflex for everyone in the organization. Awareness activities can build in these reflexes both for the security professional and for the everyday user.

Critical Success Factors for Awareness Activities

- They are based on the organization's policies
- They have senior management support
- The focus is on people at all levels of the organization
- They are effectively planned:
    - Based on user's needs, roles, and interests
    - Identifies security problems in the organization that need addressing
- They use appealing materials and methods

Awareness programs usually use repetition to reinforce desired behaviors and attitudes about security.

What is National Cyber Security Awareness Month?

National Cyber Security Awareness Month is an annual effort to increase awareness and prevention of online security problems, spearheaded by the U.S. Department of Homeland Security and the National Cyber Security Alliance (NCSA). The Higher Education Information Security Council (HEISC) promotes and participates in the annual campaign each October, joining forces with a range of organizations from the public and private sector to expand cybersecurity awareness on campuses across the country. HEISC offers many resources made by and for information security professionals in higher education.

- NCSAM Resource Kit
- Information Security Awareness Video & Poster Contest for Students
- Cybersecurity Awareness Resource Library
- EDUCAUSE Security Awareness Resource Page

How Do We Plan for National Cyber Security Awareness Month?

The following NCSAM Planning Guide worksheet (PDF or Word) will help you to think about how your institution might go about implementing a plan to take advantage of National Cyber Security Awareness Month. You can also use the Annual Campus Security Awareness Campaign, which includes monthly security awareness topics and 12 blog posts on the monthly topics with ready-made content for your campus communication channels.

Texas A&M University tries to create cybersecurity awareness campaigns that engage students in security education. For six years, they have created awareness campaigns featuring online cybersecurity games that entice more than 10,000 campus members to participate and that number continues to grow each year. Learn more about their planning process by reading their May 2017 guest blog: Bridging the Gap Between Students and Security: 7 Steps to Creating a Successful Cybersecurity Campaign.

The winning posters and videos from previous Information Security Awareness Video & Poster Contests are available for use in campus security awareness campaigns during student orientation, National Cyber Security Awareness Month, Data Privacy Day, and throughout the year.

> *Note: Videos are also available to view on the HEISC YouTube Channel. Posters can be found on the HEISC Facebook page or Pinterest page.*

If your group or institution would be interested in a presentation from an information security or privacy expert, please see our Speakers Bureau. You could also use your LinkedIn connections to invite a local, regional, or national speaker to a campus event.

Note: **Data Privacy Day** occurs each year on January 28. Think about how you might use NCSAM resources to promote this international celebration on your campus, too.

Resources

- "Building an Information Technology Security Awareness and Training Program," National Institute of Standards and Technology Special Publication 800-50, Oct. 14, 2003
- "Developing Security Education and Awareness Programs" by Shirley Payne
- DHS Stop.Think.Connect. campaign and the Stop.Think.Connect. Resource Guide
- ICANN Security Awareness Resource Locator and Security Terminology blog
- Indiana University Privacy and Security Posters
- MS-ISAC (Multi-State Information Sharing and Analysis Center) 2017 NCSAM Calendar and Posters
- NCSA Resources
- NCSAM Planning Guide worksheet (PDF or Word)
- OnGuard Online
- Presidential Proclamation: National Cybersecurity Awareness Month, 2016
- SANS Securing The Human NCSAM Planning Matrix and OUCH! Security Awareness Newsletter

State and Regional Efforts

- NASCIO (National Association of State Chief Information Officers) Cybersecurity Awareness Website

International Efforts

- **Australia**: Stay Smart Online is the Australian Government's online safety and security website.
- **Canada**: Get Cyber Safe is Canada's national public awareness campaign about cyber security and online safety.
- **Europe**: European Cyber Security Month is an EU advocacy campaign that takes place in October.
- **South Africa**: The South African Cyber Security Academic Alliance includes academic research groups from several institutions.

Questions or comments? Contact us.

⚠️ *Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).*