



## National Cyber Security Awareness Month (NCSAM) Planning Guide

This worksheet will help you think about how your institution can participate in [National Cyber Security Awareness Month \(NCSAM\)](#) and increase information security awareness on your campus. Start by answering these eight questions to help you organize and implement your campus NCSAM plan.

For additional guidance and resources, use the annual [Campus Security Awareness Campaign](#) and [Cybersecurity Awareness Resource Library](#).

### 1. *What cybersecurity awareness needs does your organization have?*

How cybersecurity-savvy is your community? Are there certain types of incidents or support issues that are occurring frequently? What are the messages you want to emphasize? Which needs are most critical?

Examples of areas you might focus on include:

- Passphrases and strong passwords
- Phishing and ransomware
- Protecting personal information
- Protecting mobile devices and laptops
- Staying safe online (e.g., social media, web browsing, good digital citizenship)
- Two-factor authentication, two-step verification, or multifactor authentication

Generally, it is more effective to identify one topic/theme each week in October, or one topic/theme for the entire month, with targeted messages sent each week.

**Our highest-priority cybersecurity awareness needs are:**

### 2. *What is your targeted population?*

Will your cybersecurity awareness efforts be aimed at the institution's entire campus community or a subset of the college or university (a school or department)? Do you want to reach everyone this year, or just one subgroup of end users? Another way to identify your intended population is to think about which group of

users may benefit the most from additional cybersecurity awareness efforts due to their level of access to sensitive data and the security risk their group's responsibilities may pose to the institution.

Examples of targeted populations include:

- General audience (entire campus)
- Technical/nontechnical
- Local/remote
- Faculty/researchers/professors
- Management/staff
- System/network administrators and support staff
- Students/parents
- Home/travel users
- New employees/contractors
- Targeted compliance training (e.g., HIPAA, FERPA, GLBA, GDPR)

As a rule of thumb, awareness campaigns that are targeted to a specific population's needs will be easier to implement and more effective in getting specific information to specific users. However, broader and more general campaigns reach more people with a "big picture" awareness message and can set the stage for more targeted cybersecurity awareness efforts throughout the year (or perhaps for next year's campaign!).

**We will target:**

**Approximate number of people:**

### *3. Is your targeted population in one geographic area or dispersed?*

One geographic location would allow for campus events such as a security fair or invited speakers, while dispersed locations may require a strategy involving e-mails, online publications, or webinars instead.

**Targeted population is located:**

### *4. What types of awareness methods tend to work with your population?*

In some communities, events such as security fairs or speaker series draw a large percentage of the population and are very effective. In others, direct mailings to individuals have the most impact. Consider which methods of communication work best in your environment. What has been successful in the past? Which methods capture the attention of the most people at your institution?

Some examples include:

- Blogs
- Bookmarks
- Brochures, business cards, checklists, tip sheets, or similar handouts
- Cartoons
- Digital messaging screens
- Escape rooms (with clues about security or privacy topics)
- Flyers
- Free giveaways (e.g., stickers, T-shirts, pens, mugs, keychains, screen cleaners)
- Movie screenings
- Online games or quizzes
- Postcards
- Posters
- Presentations (in person or online)
- Screensavers
- Social media (e.g., Facebook, Instagram, Twitter)
- Surveys
- Videos or podcasts

Additional ideas may be found in the year-round [Campus Security Awareness Campaign](#) and the [Cybersecurity Awareness Resource Library](#).

**The most effective methods for our population include:**

*5. Who is your sponsor?*

If you can indicate on all materials a number of high-level sponsors of your efforts, you will have an easier time getting people’s attention (and will likely collect more resources to assist you!). What offices or individuals might make good sponsors of this effort? Consider collaborating with other schools or departments, local nonprofits, nearby institutions, or other businesses in your community.

**Possible sponsors:**

*6. How much money do you have to spend?*

Your budget will influence many of your decisions. Remember to ask your sponsors for a contribution to the project! If you are not able to identify sponsors (or can only find in-kind contributions), determine what percentage of the information security department’s budget is available for NCSAM awareness efforts. (But don’t forget to consider your awareness budget for the entire year, not just what you plan to spend in October.)

**Our budget:**

### 7. How many people are available to assist?

How many staff from your organization can assist with this effort? Can you solicit volunteers, interns, and partnerships with departments and other institutions? As you identify staffing resources, determine each person's roles and responsibilities.

**The following people can assist in the following roles:**

### 8. How much lead time do you have?

National Cyber Security Awareness Month is observed each October. Do you have enough lead time to take on the tasks you've identified? Are there deadlines for submitting materials to your communications outlets or ordering printed materials?

If you have more lead time, you can do more! Take advantage of the year-round [Campus Security Awareness Campaign](#) maintained by EDUCAUSE, which offers ready-made content that you can easily adapt and integrate into monthly or quarterly campus communication channels.

If you have little lead time, don't give up! You can peruse the [Cybersecurity Awareness Resource Library](#) for materials to meet your needs.

Don't forget to officially show your support by signing up as a [NCSAM Champion](#) organization with the [National Cyber Security Alliance](#)—it only takes a few minutes and does not require any financial support.

**Estimated timeline:**

Find more information about EDUCAUSE [security awareness campaigns](#).