Security Awareness Detailed Instruction Manual

Last reviewed: June 2017

Handy Hint

If you're just getting started with a Security Awareness Program and you just need the basic information, check out the Security Awareness Quick Start Guide.

Other resources of interest might include the Cybersecurity Awareness Resource Library, the NCSAM Resource Kit, and the new Annual Campus Security Awareness Campaign framework and materials.

Detailed Instruction Manual (Advanced)

This guide is for campuses with an existing Information Security Awareness Program that may be able to dedicate more time and resources to developing their own materials.

Table of Contents

1) Rotate Key Messages as Monthly Themes Throughout the Year

Establishing an annual schedule for educating your community helps to deliver a more coherent message and allows subsequent communications to build on previous ones. The schedule can be based on your community's needs as identified through a risk assessment analysis, or can be based on best practices and standards. For example, you can use the following strategies:

Break the year into three topic areas as follows:

- Confidentiality (July through October)
- Integrity (November through February)
- Availability (March through June)

Each of the four month periods can be further broken down into a development cycle:

- Month One - Problem identification, topic selection, budget
- Month Two - Development of themes, materials, etc.
- Month Three - Production of materials, venue arrangement, train the trainer
- Month Four - Publish materials, conduct training/events

Selection of topics can be further fine tuned by local, national, and international trends or new requirements.

- Confidentiality - FTC Red Flags deadlines, new State Privacy Laws, reports of Social Engineering incidents, New Malware, Increase of Malicious Web Sites, Attacks on Banking Transactions, Improvements in Encryption solutions, etc.
- Integrity - Business process improvement and training opportunities during other projects, implementation of additional verification and testing procedures following discovery of problems, etc.
- Availability - Annual Disaster Recovery and Business Continuity training and planning to mitigate expected problems, debriefing and additional improvements following events such as adverse weather damage.

Another approach is outlined in the new **year-round Campus Security Awareness Campaign**, which is a framework designed to support security professionals and IT communicators as they develop or enhance their own security awareness plans. Materials include monthly security topics and 12 blog posts on the monthly topics with ready-made content for your campus communications channels. (Three dozen guest blogs developed between 2016 and 2018 are currently available.)

You can use these resources to create a steady stream of privacy and security awareness information for faculty, students, and staff. Adapt the content to make it work with your current plans and campus needs--promote each suggested topic monthly or use a 90-day awareness plan to promote a group of topics quarterly.

For additional suggested themes and ideas see the Cybersecurity Awareness Resource Library.

2) Customize a Security Awareness Website

Now that you have the basic framework for a security web site in place, it's time to decide whether to take it to the next level. While it may seem trivial, maintaining an effective web presence can be a time-consuming task. Numerous tools exist to make this process easier, but the rule of thumb is that the larger and more comprehensive the site, the work required to maintain the site is inversely proportional to the amount of effort spent on building the site and associated management tools. Review this guide, and then make decisions upfront about how much time (and money) you can invest. This will help you plan accordingly.

Key Tips and Examples

Read: Developing Your Campus Information Security Website

This document provides a great start, offering five key elements for a successful web site, plus a list of numerous other college and university security web sites.

Choose Your Battles

It's nearly impossible to fight every fight, especially on a higher education budget. There are countless security and privacy issues out there, and your site can't possibly serve as your school's comprehensive resource for all of them; there simply aren't enough hours in the day. Start to listen and learn what applies most to your constituents. Communicate with your incident response staff, and focus on content that will best fill in the security gaps at your institution.

Leverage the Rest

As the Security Awareness Quick Start Guide mentions, leverage the work of other EDUCAUSE institutions that make their work available, in addition to other non-higher ed resources, such as sites by the National Cyber Security Alliance and the U.S. Federal Government (e.g., OnGuardOnline.gov or Stop. Think.Connect.). You can find great topics and plenty of reusable content - either to link to or repurpose on your site.

Start Building

Using a Content Management System

The most effective way to maintain an updated web site is to employ some sort of web content management system. Many open-source systems are freely available, easy to setup and deploy, and have large development communities. That said, the rule of thumb applies - designing a site that makes it simple for multiple users to contribute content to and yields a more extensible framework means you'll spend a bit more time building the site infrastructure. Consider employing date stamps on information, expiration dates, or scheduled reviews of the content along with assigned roles and responsibilities to check currency of information annually, semi-annually or before the start of each academic session. Also consider using a QA tool (often offered through your web publishing group) that monitors pages for broken links, misspellings, and other minor errors.

Leveraging Social Networking and Related Media

Many security awareness professionals utilize social media, such as Facebook, Twitter, blogs, and more. These can be powerful yet easy way to connect with members of your college/university community, especially students. Tools like this bring most of the infrastructure with them, so you need only worry about the content. Remember though, most Facebook and Twitter users are used to checking in with these tools for new and updated information. If you let your content become stale, people may not feel it's worth their while to check in with your pages. Consider delegating rotating “social media duty” to a small team of employees to ensure new content is added on a regular basis.

When using social media for communications, keep in mind that these channels can also be compromised. Check security and privacy settings on a regular basis and be sure to keep track of which employees can access each account. Here is a cautionary tale from the **University of Michigan: Hacked: A Case Study**.

Location Location Location

Just as in the real world, location in cyberspace can assist you immensely. Choose an effective URL, or even better, start an information security campaign or brand and package the URL as part of that. Several institutions currently employ this approach:

- Auburn University | keepitsafe.auburn.edu/
- Baylor University | www.baylor.edu/bearaware
- Purdue University | www.purdue.edu/securepurdue
- Ohio State | buckeyesecure.osu.edu
- Rochester Institute of Technology | security.rit.edu
- Duke University | security.duke.edu
- Notre Dame University | secure.nd.edu
- Indiana University | protect.iu.edu/

If you're not quite ready to begin an entire campaign or brand, start small. A good URL will be easy to remember, type, and say verbally, such as at an event or over the phone. You may decide a brand is the way to go later (as you read through this guide), and a web site can always be redesigned or tweaked to include updated campaigns and themes.

Web Standards Can Help You

Building a site that follows good Web practices can only serve to help you, now, and in the future. Marketing and design companies try to sell people on concepts such as search engine optimization, which is really just smoke and mirrors. There's no secret or trick with modern search engines (like Google, Yahoo, or Bing) - except good, clean, well-formed HTML that complies with web standards. Other benefits of taking web standards into account are: better usability, improved accessibility for screen readers and other such devices, and an extensible infrastructure that allows you to easily repurpose your content for a wide array of audiences and consumption mediums.

Additionally, well-formed content will more easily allow for inevitable redesigns and rebranding. Remember, the more effort you put in to building a site, the greater the flexibility and robustness later on.

For more about web standards, visit:

- The Web Standards Project
- The World Wide Web Consortium (W3C)
- Open Web Application Security Project (OWASP) Top 10

3) Develop and Brand Campus-Specific Posters and Videos

Campus specific posters allow you to address those security issues that present the greatest threats at your campus. By creating posters specific to the audience, one can more effectively deliver the message. In the following examples, Purdue University staff designed a series of 50's style cartoon characters promoting safe use of computers and internet/network connectivity that were posted throughout its entire residence hall system.

- Password Poster
- Anti-Phishing Poster

When Purdue was promoting an emergency text messaging system, they featured one poster targeting the student demographic and another to market to staff and faculty.

- Student Emergency Text Message Poster
- Staff/Faculty Emergency Text Message Poster

Short informational videos are also popular and can be shared via websites, social media, or TVs on campus.

- Utah State University videos: You Are Your Own Best Defense, Don't Become a Victim, and Don't Be Fooled
- Purdue University videos: Anti-Virus PSA, Delete Unsolicited Messages, and Privacy on Social Networks

Additional materials could include postcards, bookmarks, flyers, screensavers, etc.

- Talk Like a Pirate Day (September 19)

These are just a few examples of the printed or digital materials that can be used to promote computer security awareness. For additional examples of videos, posters, and other materials created by institutions that can be modified for re-use, please visit the Cybersecurity Awareness Resource Library.

4) Develop and Brand a Campus-Specific Security (Awareness) Newsletter

Newsletters are a good way to supplement your security awareness message. Their expanded format lets you stretch out beyond incident bullets and headline splashes on home pages. They can provide in-depth explanations of current threats, promote local security initiatives, and allow you to reach you audience on a personal and emotional level through shared stories, such as dealing with identity loss after the theft of a laptop.

Getting Started

If you haven't prepared a newsletter before, begin by looking at others publications for inspiration and what might work for you (see below for some examples). For some general tips on newsletter development, read Newsletter Design and Publishing or Graphic-Designs for Hard Times and 12 Most Common Newsletter Design Mistakes from the Design & Publishing Center. Free templates like those in the Microsoft Office gallery are available to help get you started quickly.

Communicating

Form a partnership with your communications team to review and finalize the format and delivery of your important messages. IT staff provides the content and ensures accuracy of the information. The communications staff ensures readability and ease of understanding for the target audience.

Selecting a Format

A newsletter can be presented in a variety of formats. Consider your audience and resources when selecting what works best for you and your campus. Are you trying to reach a specific audience? If so, where do they get their information? Are you trying to stand out from other messages bombarding your campus? You may decide that with all of the electronic communication a hard copy of your newsletter in key offices may catch your readers' attention.

Here are examples of the most common formats. You may decide to go with one or a combination of two or more:

- Blogs: MIT's Security News, also available as a Twitter or RSS feed, or New York University's "Connect"
- Online & Print: University of Arizona quarterly newsletters (can be made available online or used to produce hard copies for distribution) or Ohio State University's IT Security News page
- Podcasts: Information Security News Podcasts produced by Northwestern University Information Technology (NUIT)

Developing Content

If your time is at a premium, consider using customizable materials from such sources as the Multi-State Information Sharing and Analysis Center (MS-ISAC). Their "Cyber Security Tips Newsletter" is produced monthly and can be readily adapted for local use.

SANS's OUCH! security awareness newsletters are another good resource. These monthly newsletters are also free and available for reprinting or sharing.

RSS feeds can provide dynamically refreshed content. One example is the MS-ISAC "Cyber Security Tips Newsletter" mentioned above. It is one of several RSS sources that Rutgers aggregates and includes on their security site.

5) Develop or Outsource Training Materials

Developing Your Own Training Materials

New Mexico State University developed in-house IT Compliance and Security Awareness training for faculty, staff, and students. More details about NMSU's approach are detailed in the EDUCAUSE Review article, "IT Compliance Framework for Higher Education."

Partner with your institution's learning and development team so your training materials incorporate best designs and techniques for adult learning and engagement. If you are interested in learning more about instructional design, consider reading 7 Things You Should Read About Innovative Approaches to Instructional Design.

Outsourcing

Learn more about third-party security awareness training tools, who might use these tools and why, as well as the benefits and risks to consider when using these tools. This resource also includes a list of technologies or tools that an institution might consider using for security awareness training efforts (e.g., PhishMe, SANS, TeachPrivacy, Wombat).

6) Build Relationships (Internal and External)

Building relationships on or off campus helps you discover resources that you may not be aware of and helps you access those resources more efficiently when you need help in time sensitive situations.

- Internal: Work with RAs, HR, internal audit, legal counsel, student leaders, researchers/faculty, and other campus departments.
- External: Contact local or national security awareness groups, professional societies (e.g., ISSA, ISACA, InfraGard, IEEE security & privacy group, FBI, local police), or student groups (e.g., ACM student chapters, physical safety & security student groups, ASIS).

7) Communicating Policies & Procedures

One critical task for IT or information security departments is communicating about campus policies and procedures. This includes highlighting the most important components of those policies, communicating with students, faculty, and staff through training or other in-person educational events, and following up with students, faculty, and staff to ensure their understanding. Also be sure to include training on how and where the client can easily look up less frequently discussed policies and standards.

Additional policy website examples:

- UVA
- Indiana University
- RIT (also refer to RIT's 2015-16 Information Security Office Communication Plan)
- University of Massachusetts
- Cornell

8) Send Community Alerts as Needed (Use Credible Sources; Keep Messages Short & Simple)

Information security alerts and advisories are used to warn the community of actual and potential threats. They can be delivered through e-mail and other traditional channels and should be incorporated into your institution's centralized messaging service when available. Avoid the temptation to be too wordy or too technical. You need to consider your audience, their attention span, and their technological "savvy."

Key Elements of an Alert or Advisory

Creating a template for your alerts and advisories will help recipients scan the information quickly

- Headline
- Tagline (teaser)
- Why the audience is receiving the message (what's the threat?)
- What your institution is doing
- What the audience should do
- Links to more information

For e-mail alerts, make sure the subject line and initial words within the message body ("pre-header") provide enough information that those receiving the email in mobile device interfaces recognize the importance of the alert and will open the message for further instruction.

Examples of College & University Alerts and Advisories:

- Brown University provides the Phish Bowl, a central repository for reports of or questions about phishing incidents.
- Princeton University also hosts a Phish Bowl on the information security office's website that shows the latest phishing alerts.
- RIT maintains an Information Security Alerts and Advisories website about recent job scams, phishing attacks, and vulnerabilities.
- The University of Rhode Island posts warnings to its Information Security Alerts page.
- The University of Arizona has a web page dedicated to phishing alerts. (For reference, see recent scam alerts from the FTC.)
- Longwood University provided an identity theft scam alert in 2013 and an eBay data breach alert in 2014.

Authenticity of Communications

An issue faced by most of us is how to ensure that the recipients know that the communications they've received are "official" and not part of a phishing attempt. We addressed this at RIT by drafting a Signature Standard that required specific elements in official communications

- RIT Signature Standard

Leveraging Social Media

To reach students, you need to go where the students are. Students are heavy users of social networking sites such as Facebook, Twitter, Instagram, Pinterest, and Tumblr. In response, many information security departments are incorporating a social media presence into their communications strategies. Use of tools such as HootSuite and TweetDeck will enable easy one-time publishing of content that you can push to different social media sites. If you are looking for timely content to share, follow the Higher Education Information Security Council (HEISC) on Twitter (@HEISCouncil) and Facebook. You can also follow other institutions such as RIT and Brown.

Information Sharing and News Resources for IT Communicators and Awareness Professionals

- APWG News
- CERT (shares recent vulnerabilities on their home page)
- Cybersecurity Nexus (ISACA)
- MS-ISAC Cyber Security Tips Newsletter
- SANS Awareness Tip of the Day
- SANS Internet Storm Center
- SANS OUCH Newsletter
- US-CERT Alerts
- US-CERT Tips
- Security Discussion Group: Subscribe to this EDUCAUSE community listserv to stay informed about information security issues in higher education.
- REN-ISAC: Join the Research and Education Networking Information Sharing and Analysis Center (please see the membership page for instructions on how to join).

9) Create and Deliver Presentations

Once you’ve developed your awareness materials and built relationships across campus, it’s time to start delivering presentations to students, faculty, and staff across campus. Here are a few ways to begin your outreach efforts.

- Summer activities for new students
- Student orientations (Note: consider including student presenters)
- Employee orientations (Note: consider adding references to important IT and security policies in the institution’s confidentiality agreements)
- Res Hall meetings
- Management meetings
- Wellness or other campus-sponsored fairs
- “Road Shows” (could be tailored to a specific audience or focus on a hot topic)

Metrics

Those with a more mature security awareness program should plan to measure their successes and record attendance numbers, as well as response rates for online quizzes, surveys, key messages, phishing campaigns, and other training efforts.

- Consider using services to train that include testing or measurement, such as “phishme.com” or the SANS phishing training/testing service.
- Offer short quizzes at the end of a training session with an offer to participate in a drawing for those show complete the quizzes.

10) Tie-In Institution or IT-Specific Glossaries Where Acronyms are Defined

The IT world can be a confusing place, filled with complex and methodical information. As a result, many common terms, processes, and names in the IT world must be equally precise - some requiring four or five words to accurately describe. This has given way to hundreds of various acronyms over the years - many that while are worlds apart in terms of functionality, can look, sound, or have very similar spellings.

The precision that computers and networks operate around constantly requires IT professionals be meticulous in nature, seldom leaving room to classify anything as minutia. For instance, when setting up a firewall ruleset, a network administrator who confused SNMP with SMTP could cause a relatively dangerous vulnerability.

The security and privacy world is no different - often requiring understanding of these IT processes and names. If your security awareness program includes more and more of these, consider using a glossary to help your users understand your documentation a bit better. It may also help them grasp a firmer understanding of the scope and/or mission of your agenda.

A few institutions have begun such projects:

- Pepperdine | Information Security Glossary
- Cal Poly Pomona | Information Security Awareness Central

Top of page

❓ Questions or comments? ℹ Contact us.