Making Security Awareness Efforts Work for You

Rebecca Fowler
Making Security Awareness Efforts Work for You

GSEC Gold Certification

Author:  Rebecca Thurmond Fowler, becky@missouri.edu

Advisor:  Charles Hornat

Accepted:  02/08/2007
Since the beginning of the field of information security, security professionals have fought a battle with user apathy and lack of knowledge. The goal of educating end users on the importance of security awareness is indeed somewhat of a “holy grail” of security. Educational institutions worldwide struggle to secure their computers and networks. While technology plays an important role in doing so, end user education is vital to securing the campus infrastructure. Many universities are recognizing the need to produce graduates well-versed in information technology and security. Degree granting programs in information technology are increasingly popular as the need for security professionals grows in the workplace. In fact, the National Security Agency encourages the certification of degree granting programs through their National Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program

“The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education in information assurance (IA), and producing a growing number of professionals with IA expertise in various disciplines.” (National Security Agency, n.d.)

However, in addition to degree granting programs, universities need to recognize their responsibility to educate the end users: faculty, staff and students who may not be majoring in or working in an IT-related field but who nevertheless need to understand the importance of information security. The value of information security awareness education cannot be overestimated. As institutions of higher education, every college has the responsibility to educate its constituents on the importance of information security, thus enabling its faculty, staff and students to effectively participate in and contribute to our increasingly digital world. In addition, protecting a campus’ information assets requires taking responsibility for the education of our users.

The Division of Information Technology, the central IT group at the University of Missouri-Columbia (MU), has implemented a comprehensive security awareness program for campus users that consists of two parts: formal awareness training and activities centered around monthly security topics. These two components work hand-in-hand; the monthly activities keep security concepts fresh in users’ minds and the training provides more in-depth information and knowledge.
At the University of Missouri-Columbia, our security awareness program began with a visit to a security professional’s conference in 2003. Despite all the interesting technical talks and presentations, what caught and held our attention was the singular importance of the average user to the security environment as a whole. In a distributed computing environment, the havoc that could potentially be wrought by one unknowing user can be almost limitless. Upon reflection, we realized that many people at the University do care about computer security – they watch the national news and read articles on the internet that impress upon them how many bad things can happen as a result of computing security incidents. However, what these users lack is the knowledge to protect themselves (and by extension, they lack knowledge of how to help protect the MU network).

People will always be the weakest link in the security chain - all it takes is one user with poor behavior or one uneducated mistake to jeopardize your security program. As security professionals, we owe it to our “joe average” users to provide education on how to behave securely in our computing environment. Especially at an institute of higher education, the need to inform people about rapidly changing security technology cannot be stressed enough.

At MU, we started with a simple premise. People need to learn about information security. From this basic principle, we realized we had to do certain things to accomplish this goal. We needed to educate users about the importance of security, and one of the most effective ways to do so is to make people realize that they have some ownership in the security process. Our information security program strives to educate users about the importance of information security topics and, as a result of this education and awareness, cause users to change their behavior accordingly.

The three broad goals of our program are:
1. To change the way people think and act when it comes to information security
2. To continually address the importance of security in the campus environment
3. To keep users informed of the rapidly changing security landscape

We set out to design a comprehensive security awareness program that would target average end users - those people who depend on computers for their work or educational activities, but who are no means computer gurus. These people make up the bulk of the university community. They need to be convinced that they should care about computer security and then they need to be educated about the specific things they should care about.
We decided to take the view of security as a “product” and market it accordingly. Our first step was to create a theme and logo that we could use to brand our product. Our initial theme was “You Are the Key to Security!” which stresses the concept that everyone participates in securing the campus computing environment. The Division of IT Marketing department helped us create a logo to carry across all advertisements we created. Our goal was to get people to associate our logo with computer security, so that any time they saw the “Key Guy” (Figure 1) they would anticipate seeing important information about computer security that they needed to pay attention to.

Figure 1.
University of Missouri-Columbia “Key Guy”

Our next step was to determine our initial list of topics that we felt needed to be addressed. We decided on a baseline security curriculum that contained information we felt every user should be exposed to. As time passes, this curriculum list grows and is revised. For example, at the inception of our program we did not include phishing in this list as we had not experienced a large problem with it at the university. However, as phishing became more prevalent information about phishing scams and how to protect yourself ended up being moved into the base curriculum. (Anti-Phishing Working Group, 2005) Repetition is the key to keeping the base curriculum in the forefront of people’s minds. For example, the Digital Millennium Copyright Act (DMCA) (U.S. Copyright Office, 1998) is a very important issue for us to address, as many students choose to illegally share copyright music and movies. We address this issue every August/September and every January/February to coincide with the start of the academic semester. This means that a student who is enrolled at MU for 4 years will see the material 8 times. However, it also means that if a student doesn’t enroll until our winter semester (which starts in January) that they will see the information immediately and not go through an entire semester without being informed about the DMCA requirements and consequences. In an educational institution where faculty, staff, and students pass through on a regular basis you must
Making Security Awareness Efforts Work for You

continually address the base curriculum in order to hit all of your target audience.

At MU, our current base security awareness curriculum consists of:

• Password safety and security
• E-mail safety and security (including phishing scams, spam, abuse, and harassment issues)
• Desktop security (including antivirus, OS and application updates, and spyware)
• FERPA issues (the Family Educational Rights and Privacy Act is a federal law that governs the release of student information in an educational institution) (U.S. Dept. of Education, n.d.)
• Acceptable Use Policy

These issues are addressed on a regular basis with all faculty, staff and students. The base curriculum is communicated via free online and in-person training sessions. We developed an online course using WebCT that users can sign up for and work through at their own pace. We also provide in-person training to departments or students groups who are looking for a speaker to discuss computer and information security. To date, we have formally trained over 1400 faculty, staff and students with our base curriculum. There are efforts underway in many departments to require the training as a condition of employment or as a homework requirement for a student’s for-credit course. Formal training gives us an opportunity to provide a captive audience with the information they need to know to practice safe computing.

However, in addition to the base curriculum, there are also special “hot topic” items we want to inform our users about. This can include anything from severe security issues or incidents we’re dealing with to time-sensitive, security-related information. For example, in the April/May timeframe of every year we do a marketing push on the importance of making backups of your data. We tie this to end of semester issues such as term papers and dissertations, and use the importance of being able to turn your paper in on time as an example of why it’s important to keep multiple copies of your data. Another time-sensitive marketing push we conduct in November/December of each year is to publicize suggestions on how to shop safely online. This coincides with the holiday buying season and helps users relate computer security topics to their everyday lives.

The “hot topic” items may be addressed during in-person training, but more frequently they are marketed using a variety of avenues of distribution. Some examples include campus display cases, newsletter and newspaper articles,
Making Security Awareness Efforts Work for You

table tents in dining halls across campus, and poster campaigns. By working with a variety of campus departments, including the Student Commons, the student newspaper, the Library Information Commons, and the College of Education CCTV network we are able to leverage existing advertising opportunities to promote our security awareness message. Examples of a variety of branded marketing materials are available in the appendices.

One of the most challenging parts of conducting an effective information security awareness campaign is designing and collecting metrics. Measuring the effectiveness of various efforts can be costly and time consuming, but it must be done if you want to ensure that you are reaching your target audiences. The University of Missouri currently measures metrics quantitatively by tracking the number of users who attend in-person or web-based security awareness training. We are moving toward a model where more qualitative methods of assessment will be used, such as online quizzes to measure knowledge retention, random inspections to assess the implementation of workplace security guidelines, and departmental audits to provide a true picture of a department’s security posture both before and after exposure to security awareness materials. Determining from the beginning of your program what criteria you will measure and how you will measure it will allow you to gauge the success of your awareness efforts. After each substantial marketing push you can return to your metric criteria and judge the effectiveness of your efforts. This will allow you to make adjustments to your message and method of delivery to obtain the best results for your environment.

In closing, getting your users to know and care about information security can definitely be a challenging task. Identifying a theme can help you craft a cohesive program that looks professional and helps users instantly recognize your message. Determining the concepts you would like users to understand should also be a priority, as you must focus your efforts on the topics that are most important in your environment. Finally, repetition is the key to getting your message across. Security awareness messages should be conveyed on a regular basis and in a variety of mediums so that maximum exposure to your message can be achieved.
Making Security Awareness Efforts Work for You

References


Appendices

University of Missouri Branded Security Awareness Materials

Appendix 1: Brochure advertising security-related services, with specific paragraph regarding in-person and web-based security awareness training. Distributed in residence halls, front desks, libraries and student commons.

Appendix 2: Identity theft table tent. Placed in table tents on all tables in all campus dining hall facilities.

Appendix 3: Postcard advertising Annual Cyber Security Awareness Day event. Distributed via campus mail to all students living in residence halls and all faculty and staff. Image was also used as a web page advertisement on the main campus web page.

Appendix 4: Payroll stuffer, placed in all campus employee’s payroll stubs (including student employees). Distributed with November paycheck (received by users in early December).
Appendix 2:

WHAT'S THE FASTEST-GROWING CRIME IN THE US?

IDENTITY THEFT!

Don't be a victim!
Learn how to protect yourself.

latservices.missouri.edu/safe-computing/
Appendix 3:

2nd Annual
Security Awareness Day 2005
October 27, 2005 • 9 am – 5 pm • Memorial Union

Join IAT Services for this free, one-day workshop!

- Identity Theft
- Phishing Scams
- Workstation Security
- Information Security at MU
- Virus Protection
- Vendor Fair

Registration is required and automatically registers you for drawings.

iat/services.missouri.edu/safe-computing/awarenessday05.html
Appendix 4:

This Holiday Season,

Shop Safely Online

Know who you’re buying from.
Only make purchases from reputable vendors.

Know exactly what you’re getting.
Make sure you read the item description carefully.

Check the delivery date.
Get it in writing to avoid any misunderstandings.

Use a secure Web browser.
Make sure the URL starts with “https”.

Always read the return policy.
For more safe online shopping tips, visit
iat.services.missouri.edu/safe-computing/

If you do experience problems with online
shopping, file a complaint with the Missouri
Attorney General’s Office by visiting
www.ago.state.mo.us/forms/complaintform.htm.
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Chicago Spring 2020</td>
<td>Chicago, ILUS</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit &amp; Training 2020</td>
<td>Munich, DE</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Budapest June 2020</td>
<td>Budapest, HU</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas Summer 2020</td>
<td>Las Vegas, NVUS</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich June 2020</td>
<td>Zurich, CH</td>
<td>Jun 15, 2020 - Jun 20, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London June 2020</td>
<td>OnlineGB</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>