



FISSEA Security Awareness, Training, & Education Contest

Entry Form

Please review rules before completing entry form including the due date. No late entries will be accepted. E-mail entries to fissea-contest@nist.gov.

Name of submitter: Chrisan Herrod

Organization: University of Maryland University College

Address: 4716 Pontiac Street
College Park, Maryland 20740

Phone: 301-985-7073

Email Address: Chrisan.Herrod@umuc.edu

Type of Entry:

Awareness: there are four categories in this area: Poster, Motivational Item (aka: trinkets - pens, stress relief items, t-shirts. etc.), Website, Newsletter

Training & Education: there is one category for this area: Interactive scenario/exercise

Motivational Item

Title of Entry: Get Stuck on Security

Description of Entry:

In observance of 2012 National Cyber Security Awareness Month, UMUC designed a series of messages that addressed four key security practices (password strength, phishing, cloud security, and computer use). UMUC highlighted one security practice for each week in the month of October. The messages were available through a variety of media outlets, newsletter, emails and internal website. Magnets were designed to highlight each of the four key messages. The magnets were given as handouts to participants of UMUC's Cyber Security Awareness Day Conference.


Each magnet contained the familiar image associated with the security practice. The “Pick Powerful Password” message was captured on a magnet which featured simple emoticons suggesting strong password versus weak password. This magnet served as a reminder to create strong passwords.

- Include at least eight characters in a mix of upper and lower case letters, numbers, and special characters
- Don’t use names of family members, favorite pets, birthdays, or anything that could easily be looked up
- Add parenthesis and even a weak password will become much stronger
- Change passwords every 90 days, and replace at least half the characters instead of just rearranging them

The second message “Elude the Evil E-mailer” featured a devil email image that reminded users to be cognizant of phishing attacks. The messaging included an emphasis on avoiding attacks:

- Consider the legitimacy of an e-mail before replying, opening an attachment, or clicking on an embedded link
- Don’t provide password or other personal information if you do not recognize the source of the e-mail
- Verify that messages are really from who they say they are ... especially if you have any doubts.

The third message converted to a magnet was the “Log Out to Lock Out Trouble” that featured a laptop image with a lock image imbedded in the screen. This message reminds the user to log out in order to secure information and prevent loss and damage. The message provides the tips:

- Make it a habit to log off your computer whenever you get up, even if you’ll only be away a few minutes
- Learn the keyboard logoff shortcuts for your computer: Ctrl+Alt+Del on a PC;  ⌘ Q on a Mac
- Don’t leave your password on a sticky note stuck to your screen where villains can find it
- Close and lock your office door, too, as a second line of defense

The fourth message “Beware of the Leaky Cloud” enforces security safety while on social media sites. This message features an image of a unhappy cloud with tear drops. The message reminds users to restrict posting of private, personal, or sensitive data on social networks with public access and emphasized the following:

- Accept only those third-party applications permissions that come from trusted sites to avoid infection by malicious apps that can use social networking site access to steal and misuse personal data
- Enable the encryption feature (called HTTPS) on any Web site that offers this as an option
- Be careful when clicking on links in e-mail messages that claim to originate from a social networking site or links posted on people’s walls or public pages

- Use caution if a friend or stranger requests money or makes a surprisingly good offer on a social network, because criminals often use the open nature of such sites to defraud others

And finally, a fifth magnet was design to capture all four security message on one display.



LOG OUT TO LOCK OUT TROUBLE

U are the center of SEC_RITY at



PICK POWERFUL PASSWORDS

U are the center of SEC_RITY at



BEWARE OF LEAKY CLOUDS

U are the center of SEC_RITY at



ELUDE THE EVIL E-MAILERS

U are the center of SEC_RITY at





PICK POWERFUL PASSWORDS



LOG OUT TO LOCK OUT TROUBLE



ELUDE THE EVIL E-MAILERS



BEWARE OF LEAKY CLOUDS

U are the center of **SEC_RITY** at



UMUC

University of Maryland University College