



Enrich Your Security Awareness Training

Get Compliant.
Get TraceSecurity.

Objectives

This educational webinar will offer expert guidance on several topics, including:

- 1. Establishing the fundamentals of a security awareness training program**
- 2. How to successfully communicate the staff's role in combating specific security threats like Social Engineering and ID Theft**
- 3. Crafting memorable real-world examples for training purposes**

Common dilemma

How do you deploy an effective security awareness training program that:

- 1. Addresses the needs of the organization**
- 2. Impacts staff members**
- 3. Also meets regulations**

Challenges facing trainers

- **Moving security awareness to a higher priority within the company**
- **Delivering a consistent message about the importance of information security**
- **Developing training materials that deliver a clear and memorable message**
- **Getting the “buy in” from staff**
- **Ensuring the training meets compliance regulations AND can be documented!**

So what are the requirements?

GLBA (Gramm-Leach-Bliley Act) requires that certain organizations must develop and implement an appropriate information security program based upon size, nature and sensitivity of organization:

- To ensure the security & confidentiality of customer data.
- To protect against any reasonably anticipated threats or hazards to the security or integrity of such data.
- To protect against unauthorized access to or use of such data that would result in substantial harm or inconvenience to any customer/member.

Key components of an awareness program:

- All employees must be regularly or continually exposed to *information security awareness* messages.
- All users of information and information systems must attend *information security awareness training* once per year.
- Each person who has been identified by his or her organization as having significant responsibility for information security must receive formal *role-based information security training*.

Who is at risk?

People at all levels are at risk...
This includes EVERYONE!

IT STAFF

CALL CENTER

MANAGEMENT

TELLERS

LOAN OFFICERS



BACK OFFICE

MARKETING

PROCESSORS

ADMIN STAFF

JANITORIAL CREW

This image is included in our FREE Security Awareness Toolkit!

The Human Factor

Criminals tend to seek out the weakest link in security...many times, this is the HUMAN FACTOR

Security Awareness Training helps mitigate threats

- **Protecting Your Network from Outbound Threats**
- **Protecting Perimeter Security from New Hacking Techniques**
- **Combating the Threat of Social Engineering**

Motivating factors for learning

- **Memory Persistence** – Cite current news stories or recent situations that affected the organization to help reinforce the consequences of security lapses
Tip: Purge outdated stories no matter how “relevant” they may seem to be.
- **Value of Perceived Importance** – People tend to adhere to rules that are deemed the most important.
Tip: Keep Security Awareness “Top of Mind” through multiple techniques
- **Self Sufficiency** - People are more inclined to follow procedures that they understand AND feel do not hinder their productivity.
Tip: Emphasize training on procedures most important to the organizations; i.e. password creation and usage

Motivating factors for learning

- **Self Interest - People are more receptive to information that affects them personally or that they can relate to**
Tip: show how security awareness can translate into safety in their personal life

Good Example to reinforce keeping passwords inaccessible:

***You wouldn't jot down the
PIN for your home alarm
on a sticky note and then
stick it right on the keypad...
would you???***



This image is included in our FREE Security Awareness Toolkit!

Guidelines for delivering the message

How do we get the desired results?

- Build interest
- Educate
- Communicate
- Repeat

Guidelines for delivering the message

- Make it easy for the audience to “buy-in” to the message
- Remember the **WIIFM rule**: *What’s In It For Me?*
- Make sure the information is delivered in a manner that appeals to the individual as being valuable to them *personally and professionally*.
- Give them partial ownership of the process by stressing how important each individual is to the overall security culture

HINT: When possible, train employees of similar levels in groups. This allows a trainer to tailor a message based on the interests and experience level of the audience.

Communicating the message

Clearly communicating the message, plus continuously reinforcing the message is the key to a successful security awareness program!



To do so, you may need some creative tools and techniques to supplement your existing program

TraceSecurity provides a Security Awareness Toolkit to help you out!

Helpful Tools and Techniques

- **Catch Phrases and Slogans**

"Control + Alt + Delete When You Leave Your Seat"

"Don't Get Hooked by Phishers...Think Before You Click"

- **Creative Training Exercises**

Simulated Game Shows

Create-A-Password exercises

More examples are
included in the FREE
Security Awareness
Toolkit!

- **"Real-Life" Scenario Discussions**

You come back from lunch to find a door that should be secured is propped open and there's a note stating "Pizza Person: Bring the pizzas to room 755". What should you do?

Continuously reinforce the message

- Screensavers
- Inter-office Email Blasts
- Intranet Banner Ads

Our FREE Security Awareness Toolkit includes a collection of screensavers and web banners!



Continuously reinforce the message

Posters are a recommended technique. TraceSecurity makes these posters available for FREE!



Helpful Tools and Techniques

Utilize an electronic training system

Improves process of disseminating and tracking information

Host Special Events

A company-wide buffet, courtesy of the "Security Awareness Team"

Develop POSITIVE Internal Case Studies

Look for "teachable moments" where an employee made the right decision in Detecting, Protecting or Reacting to a threat

Security Recognition Awards

Develop Security Watchdogs, or "Human Firewalls"

Helpful Tools and Techniques - News Stories

Show videos of news reports concerning social engineering techniques

(A Google search should yield a variety of useful results)

Monitoring News Aggregation sites will help build a “bank” of real-world examples

(Most sites allow you to set up filters to identify content)

Send links to these stories out in internal newsletters or email blasts

(Be sure to also include your internal message!)

Helpful Tools and Techniques – “Hot Topics”

Password Creation Techniques

Be careful...some of the “most common” techniques of teaching password security are outdated!!!

Social Engineering Tactics

Continuously remind staff about common tactics like Tailgating, Another, Another

Social Networking Risks

What happens in cyberspace doesn't necessarily stay in cyberspace!

Maintaining and improving the program

- **Continuously monitor the success of the program**
- **Security Awareness “Case Studies”**
- **Allow employees to provide honest feedback**
 - **Evaluation forms**
 - **Web-based evaluations**
 - **Pre and Post testing**
 - **Feedback from management**

Reinforce the culture

- **Make security threats seem real and pertinent, make it believable.**
- **Use social marketing techniques to encourage safe practices; make security interesting.**
- **Make security less of a hurdle to productivity; show how unsafe practices and shortcuts can actually hinder productivity by introducing risks.**
- **Don't fall victim to the "Do as I say and not as I do" trap; enforce security policies fairly and consistently**
- **Security Awareness Training is not a one-way knowledge transfer; be open to feedback on the effectiveness of the program.**

Recognizing “Awareness Champions”



This logo is included in our FREE Security Awareness Toolkit!

- T-Shirts
- Office Plaques
- Newsletter Profile



Summary

- **Deliver security information that users will view as being valuable to them personally and professionally**
- **Communicate with users, let them know why policies exist and why they are enforced for everyone**
- **Be mindful of security solutions that can impact usability and communicate the need to users whenever such solutions are implemented**
- **Remember that security awareness isn't a one shot fix but a long term process designed to educate AND to change user behavior**
- **Communicate OFTEN and through different media**

FREE Security Awareness Toolkit

A collection of free content you may use and/or modify to suit your needs, including:

- **High Resolution Posters**
- **Web Banners**
- **Computer Wallpapers**
- **Training resources**

The link will be emailed to attendees after the conclusion of this webinar!

www.tracesecurity.com/solutions/security_training.php

Contact Info:

Brady Justice
brady@tracesecurity.com
225-612-2125

www.tracesecurity.com

TraceSecurity is
CUNA's EXCLUSIVE
provider of security
compliance assessments.



- Security Assessments
- Risk Assessment
- IT Security Audits
- Penetration Testing
- Social Engineering
- Security Training
- Application Testing

www.tracesecurity.com