Topic: Social Engineering Date: _____

Trainer Checklist

	Task	Date Completed
1.	Print Trainee Checklist, fill in employee names.	
2.	Review objective and training materials on the social engineering web page at **https://sites.google.com/site/kissatisat/topics/socialengineering**.	
3.	Choose one or more methods for employees to learn about social engineering.	
4.	Communicate requirement to employees to complete training.	
5.	Verify employees know to provide information only to authorized individuals and can recognize the signs of a social engineering attempt.	
6.	Document employee progress on Trainee Checklist and/or ISA Training Checklist.	

Topic: Social Engineering _____ Date: _____

Trainee List

Employee Name	Supervisor/Department	Trainer Initials
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		

Topic: Social Engineering **Date: _____**

Lesson Plan

Objective: Recognize social engineering attempts

How to protect against Social Engineering:

1. Providing sensitive information to strangers pretending to be a part of the organization should be avoided. Any such activity should be reported to the management.
2. Employees should be trained against social engineering attacks from in-person, phone, e-mail, or other electronic methods.

Source: *Small business information security workbook, version 2.2*. Lincke, 2011.

Teaching tip: Talk about possible social engineering situations that may happen at work.

1. Dangers
   a. "Amateurs hack systems, professionals hack people" (Mellor & Noyes, 2005).
   b. A password or any other confidential information is only as confidential as people are willing to keep it.
   c. Social engineers often prey on sympathy or desire to avoid conflict.
2. How to combat Social Engineering
   a. Social engineering is an attempt to manipulate legitimate users to gain unauthorized information.
   b. Always be aware of who you are communicating with and what information they are requesting from you.
   c. Don't give out information (no matter how insignificant it seems) to someone who isn't authorized to know it.
   d. Don't offer supplemental information that is not necessary.
   e.g. If Linda is gone for the day and someone calls up and asks if she is in, don't tell them that she always takes the third Friday off. Just tell them she is not in. Be aware and be careful.

Note: The material contained in this lesson plan was adapted from the case study "Awareness and Accountability in Information Security Training" (Mellor & Noyes, 2005) and used with permission.

Topic: Social Engineering _____ Date: _____

Lessons

Title	URL	Duration
InfraGard Awareness Information Security Awareness Training Course – Lesson 3 How your behavior can be exploited	https://www.infragardawareness.com	9 Minutes, 56 Seconds
InfraGard Awareness Information Security Awareness Training Course – Lesson 5 Understanding and avoiding social engineering	https://www.infragardawareness.com	4 Minutes, 5 Seconds

Podcasts

- Getting in Front of Social Engineering - http://www.cert.org/podcast/show/20080429hinson.html

Posters

- Social Engineering Awareness - Poster – http://www.sans.org/security-resources/policies/desk-top.php

Reading

- A Tried and True Weapon: Social Engineering - http://securingourecity.org/resources/whitepapers/Social_Engineering_Borghello.pdf

Policy Templates

- Social Engineering Awareness Policy – http://www.sans.org/security-resources/policies/desk-top.php