<Company Name>

SOCIAL ENGINEERING AWARENESS
Employee Front Desk Communication & Awareness Policy

Created for SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send an e-mail to stephen@sans.edu.

1.0 Overview

1.1 The Social Engineering Awareness Policy bundle is a collection of policies and guidelines for employees of <Company Name>. This Employee Front Desk Communication Policy is part of the Social Engineering Awareness Policy bundle.

1.2 In order to protect <Company Name>'s assets, all employees need to defend the integrity and confidentiality of <Company Name>'s resources.

2.0 Purpose

This policy has two purposes:

2.1 To make employees aware that (a) fraudulent social engineering attacks occur, and (b) there are procedures that employees can use to detect attacks.

2.1.0 Employees are made aware of techniques used for such attacks, and they are given standard procedures to respond to attacks.

2.1.1 Employees know who to contact in these circumstances.

2.1.2 Employees recognize they are an important part of <Company Name>'s security. The integrity of an employee is the best line of defense for protecting sensitive information regarding <Company Name>'s resources.

2.2 To create specific procedures for employees to follow to help them make the best choice when:

2.2.0 Someone is contacting the employee - via phone, in person, email, fax or online - and elusively trying to collect <Company Name>'s sensitive information.

2.2.1 The employee is being "socially pressured" or "socially encouraged or tricked" into sharing sensitive data.

3.0 Scope

Includes all employees of <Company Name>, including temporary contractors or part-time employees participating with help desk customer service.

4.0 Policy

4.1 Sensitive information of <Company Name> will not be shared with an unauthorized individual if he/she uses words and/ or techniques such as the following:

4.01.0An “urgent matter”

4.01.1A “forgotten password”

4.01.2A “computer virus emergency”

4.01.3Any form of intimidation from “higher level management”

4.1.4 Any “name dropping” by the individual which gives the appearance that it is coming from legitimate and authorized personnel.

4.1.5 The requester requires release of information that will reveal passwords, model, serial number, or brand or quantity of <Company Name> resources.

4.1.6 The techniques are used by an unknown (not promptly verifiable) individual via phone, email, online, fax, or in person.

.7 The techniques are used by a person that declares to be "affiliated" with <Company Name> such as a sub-contractor.

4.1.8 The techniques are used by an individual that says he/she is a reporter for a well-known press editor or TV or radio company.

4.1.9 The requester is using ego and vanity seducing methods, for example, rewarding the front desk employee with compliments about his/her intelligence, capabilities, or making inappropriate greetings (coming from a stranger).

5.0 Action

5.01.0All persons described in section 3.0 MUST attend the security awareness training within 30 days from the date of employment and every 6 months thereafter.

5.01.1If one or more circumstances described in section 4.0 is detected by a person described in section 3.0, then the identity of the requester MUST be verified before continuing the conversation or replying to email, fax, or online.

5.1.2 If the identity of the requester described in section 5.1.1 CANNOT be promptly verified, the person MUST immediately contact his/her supervisor or direct manager.

5.1.3 If the supervisor or manager is not available, that person MUST contact the security personnel.

5.1.4. If the security personnel is not available, the person described in section 3.0 MUST immediately drop the conversation, email, online chat with the requester, and report the episode to his/her supervisor before the end of the business day.

6.0 Enforcement

6.1.0 All persons described in section 3.0 who (a) successfully detect circumstances set forth in section 4.0 and (b) correctly complete an action described in section 5.0 are entitled to have an extra day off at the discretion of their direct supervisor or manager.

6.1.1 All persons described in section 3.0 who violate this policy may be subject to temporary suspension from work and must attend <Company Name>'s security awareness training again before being readmitted.

7.0 Revision History

7.1.0 Policy is in effect starting July 16, 2009; Version 1.0, Emilio Valente

7.1.1 Document revised (date, version and author): _____