Homework Assignment 4: Social Engineering

Matthew Austin

Fontbonne University

Quagliata

25 October 2016

**Social Engineering Awareness Policy**

***1. Overview***

This Social Engineering Awareness Policy is a collection of policies and standards for users/employees of our organization. In order to insure the our organization's resources are safeguarded, all users/employees have to protect the integrity and confidentiality of our assets.

***2. Purpose***

This policy informs employees to make this aware of social engineering threats and attacks, along with teaching them ways to notice when there is a social engineering attack is eminent.

Users/Employees will be information of multiple techniques depending on the type of attacks that are used to better understand them and will be given standard rules to respond to such attacks. In the event that the attack is out of their control they will know who to contact (recommended that it is someone of higher privilege in the organization). The user/employee will know that they are the main weakness but also the main line of defense against social engineering attacks.

User/Employees will finally be informed on what to do when someone is contacting them (in any medium) and are try to retrieve sensitive information and will also be informed on what to do when the employee is being socially pressured and/or tricked into sharing important information.

***3. Definitions***

**Social Engineering:** the application of sociological principles to specific social problems.

**Communication (via any medium)** - communication through phone, email, online, fax, or in person

**Chief Security Officer** - Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and 3) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

**Phishing** - Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.

**Malware** - A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.

**Trojan Horse (via Digital and Physical)** - A computer program or person that appears to have a useful function, but also has a hidden and potentially malicious function or person that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program or person.

***3. Scope***

This policy applies to all employees of our organization, including temporary/full-time contractors and part-time/full-time employees participating in any action within the organization.

***4. Policy***

4.1 Important information of the organization will not be shared with an unauthorized (and sometimes even “authorized) individuals if the person uses words and techniques (through any medium of communication) such as:

* An “urgent matter”, “forgotten password”, and or “computer virus emergency”.
* Intimidation using statements that are or are similar to “higher level management”, and or “name dropping” without getting contacted by the actual higher privileged authorities our organizations secure procedures state.
* The person that wants information wants that contains sensitive information such as passwords, SSNs, ID’s, and other important information.
* The person who wants information claims to be from a “contractor” or “reporter” (from news/press of any medium) affiliated with the organization without getting any notice from higher privileged authorities our organizations secure procedures state.
* The person who wants information uses ego and/or vaniity seducing methods such as rewarding an employee with compliments about their intelligence, capabilities, or making inappropriate greetings and comments that would be seen as “charming”.

4.2 All employees will take these actions to ensure that they are rightfully informed about and are capable of mitigating social engineering attacks:

* All user/employees are to attend security awareness training within 7 days after they are initially employed and every 3 months after.
* If a social engineer attack circumstance arises and is detected, then the identity of the person requesting information must be verified (using the proper procedures created by the Chief Security Officer or Data Monitoring Committee) before proceeding with the interaction (through any medium).
* If the identity of the person requesting information can not be verified, the person the requester is interacting with must immediately contact and inform their supervisor, direct manager, or anyone of higher authority.
  + If a person of higher authority is not available, the person must contact security personnel.
* If security personnel is not available, the person must immediately discontinue the interaction via any medium of communication with the person whom requested information, and report the event to the supervisor or person of higher authority before the end of the business day.

**Reference**

Campus Information Technology Security Policy. (2016). Retrieved August 22, 2016,

from <https://security.berkeley.edu/campus-information-technology-security-policy>

<https://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-example-data-security-policies-na.pdf?la=en>

The University Policy Manual. (2016). Retrieved August 22, 2016, from

<https://policy.uncg.edu/university-policies/data/>

Secure The Breach | Get Ready For A Security Breach. (n.d.). Retrieved August 30,

2016, from <http://www.securethebreach.com/encryption.html>

Information Security | Washington University in St. Louis. (2016). Retrieved August 22,

2016, from <https://wustl.edu/about/compliance-policies/computers-in>

Kissel, Richard. *Glossary of Key Information Security Terms*. N.p.: n.p., n.d.*Glossary of Key*

*Information Security Terms*. NVL Publications. Web. 32 Oct. 2016. <<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>>.

SANS. "Social Engineering." *Consensus Policy Resource Community*. SANS, n.d. Web. 23 Oct.

2016. <<https://www.sans.org/security-resources/policies/retired/pdf/social-engineering-awareness-policy>>.