

IT Security Standard:

Social Engineering

Introduction

This standard defines the specific steps needed to implement Bellevue College policy # 5250: *Information Technology (IT) Security* and other policies and standards as they relate to the information technology attack strategy known as “Social Engineering.” This standard is necessary to help assure the integrity and reliability of the Bellevue College internal networks, the computers on those networks, and the software installed on those computers, and is meant to provide an outline of detecting and combating social engineering methods. The standard will be reviewed annually or when changes are implemented.

Scope

This document is intended to augment, not supersede any Bellevue College IT security policy. It intends to help define the attack strategy known as social engineering and provide guidelines for educating employees about prevention methods and the value of the information they use on a daily basis.

Social engineering attacks can have either a physical or psychological component. The physical aspect encompasses such things as the workplace environment, use of the phone, going through trash or view proximity to the employee. The psychological component is based upon creating an environment of persuasion or trust, through impersonation, ingratiation, threats and/or friendliness.

Exceptions

A variety of exceptions to this standard may be expected. These exceptions, when granted, will be documented in either a platform specific standard or in a memo documenting the exception. Exceptions may be granted by the Bellevue College IT Security Administrator, the Dean of Information Resources (IR), or any IR director authorized by the Dean. Copies of all documentation regarding exceptions will be kept on file with the Bellevue College IT Security Administrator. This documentation will include:

1. A detailed description of the exception.
2. A description of why the exception is necessary.
3. A risk assessment by the Bellevue College IT Security Administrator and/or the Dean of Information Resources, or designee.
4. A description of the compensating controls that are in place to mitigate risk created by the exception.

Business Impact and Risk, Threat and Vulnerability Analysis

Social engineering is the manipulation of the human tendency to trust in order to break into computer networks or gain unauthorized access to information or computing resources. Social engineering was one of the earliest successful hacking techniques, and was first addressed by the CERT internet security research and development center in their Security Bulletin CA-1991-04.

Since it relies on the cooperation of college computer users, who are unpredictable in their responses and often trusting and helpful, it is one of the greatest security threats. It provides the attacker a way to bypass all electronic security methods.

Damage that could be sustained includes:

- Unauthorized access to data -- malicious
- Unauthorized modification of data -- malicious
- Theft of equipment or resources -- malicious

- Damage to equipment or resources -- malicious
- Denial/loss of service -- malicious
- Loss of reputation

The goal of this standard is to prevent intrusion by outside parties through the unwitting collaboration of Bellevue College employees. Once access is attained, severe damage could be done to the any or all college network and computing systems.

Standard

A. Introduction

1. The main purpose of social engineering, a term that was coined by computer hackers, is to obtain a user's password. Any account which provides access to the Bellevue College computers or network can be used by a knowledgeable user in many malicious ways, the least of which compromise only the account for which the password is known. With the correct software tools and patience, a sophisticated hacker can use an account with very few security rights to eventually elevate their way into the main campus servers, thus compromising every account on the network.
2. A secondary risk related to social engineering is to physically obtain sensitive information or gain access to unattended systems, thus negating the need for a password.
3. The first line of defense is to understand that social engineering attacks include both physical and psychological methods, and usually have 4 distinct elements:
 - a. Information Gathering,
 - b. Relationship Development,
 - c. Relationship Exploitation, and
 - d. Objective Execution.
4. Physical methods for collecting information may include:
 - a. Impersonation of repairmen, IT support, managers, etc. either by phone or in person.
 - b. Dumpster diving, to collect and analyze information from trash.
 - c. "Shoulder surfing," to see employees type their passwords.
 - d. Searching a work area for passwords or other sensitive information that has been written down.
 - e. Using computers that are already logged-in.
5. Psychological methods of collecting information depend upon the assumption of trust and manipulate emotion to acquire information or access. Many times the interaction can be by phone or email, and include:
 - a. Direct phone requests to Helpdesk for password resets.
 - b. Pleas or threats for information by impersonation of authority figures or support personnel.

B. Awareness

1. Social engineering relies fundamentally on the victim's willingness to trust or help other people. In a service-oriented environment, this trust creates a significant challenge to staff and requires they are constantly on guard. Awareness of various methods used to gather information is an imperative step in maintaining security.
 - a. Campus employees are expected to be familiar with Bellevue College policies and IT security standards prescribing what may and may not be released to outside parties, and these should always be followed.

- b. Bellevue College has a responsibility to provide a security awareness program providing information regarding security policies and practices.

C. Suggested Responses

1. Responses designed to limit social engineering opportunities can be implemented at both the campus and office level. Important precautions include:

Area of Risk:	Malicious user Tactic:	Strategy to combat risk:
Dumpsters, office trash	Dumpster diving	<p>Once something is left for trash, there is no expectation of privacy.</p> <ul style="list-style-type: none"> • Reports containing sensitive data will be shredded before disposal. • All computer system media (Floppy disks, CD-ROM disks, Tape, Hard drives [Internal or External], computer systems) will be disposed of following the procedures listed in the "Media Disposal" IT security standard.
General-Psychological	Impersonation & persuasion	<ul style="list-style-type: none"> • Maintain awareness and training programs • Challenge the authority or identity of persons unknown to you – ask them to identify themselves. • IT support personnel will wear Bellevue College identification.
Bellevue College Network, E-mail, Internet Usage	Creation & insertion of trojan software to acquire passwords or other sensitive information	<ul style="list-style-type: none"> • Continual awareness of system and network changes by support personnel. • Training on password use and management. • Campus user awareness regarding e-mails from unknown senders and e-mails with attachments.
Server rooms / Phone closets	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab confidential data	<ul style="list-style-type: none"> • Keep phone closets, server rooms, etc. locked at all times (REF: Bellevue College IT Security Standard addressing <i>Physical Security</i>). • Keep updated inventory on equipment. • Do not allow anyone but authorized staff, and escorted guests into restricted areas of buildings.
Mail room	Insertion of forged memos; Theft of mail	<ul style="list-style-type: none"> • Lock & monitor mail room
Offices	Shoulder surfing; Stealing sensitive documents; Wandering through halls looking for open offices; Using vacant computers that are already logged-in	<ul style="list-style-type: none"> • Don't type in passwords with anyone else present (or if you must, do it quickly!). • Mark documents as confidential & require those documents to be locked. • Require all guests to be escorted. • Do not store or post passwords near computers. • Lock computer when user not present, even for a "minute".
Phone & PBX	Stealing phone toll access	<ul style="list-style-type: none"> • Control overseas & long-distance calls. • Protect Scan codes as passwords.
Help Desk	Impersonation; persuasion	<ul style="list-style-type: none"> • Help Desk should give out passwords only upon verification of individual identification.

Sanctions

Violations of the provisions of this, or any Bellevue College IT security standard or policy, will be dealt with immediately in the same manner as any violations of Bellevue College policies, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:

1. Permanent loss of computer use privileges;
2. Denial of future access to Bellevue College IT resources;
3. Disciplinary action – any disciplinary action will be taken in accordance with appropriate procedures as established by the Vice President of Human Resources (for employees) or the Associate Dean of Student Success (for students);
4. Dismissal from the college; and/or
5. Legal action.

Those users who misuse or abuse any computing or network resource may have their login accounts closed and access to the systems immediately terminated. Some violations of this standard may also constitute a state, local, or federal criminal offense.

Appendix A – References

1. Bellevue College Policy #5250: *Information Technology (IT) Security*
2. Bellevue College IT Security Standard: *Physical Security*
3. Bellevue College IT Security Standard: *Media Disposal*
4. Bellevue College IT Security Standard: *Password Management*
5. SBCTC-IT IT Security Standard: *Social Engineering*
6. SecurityFocus, Sarah Granger, *Social Engineering Fundamentals, Part I Hacker Tactics*, December 18, 2001
7. SecurityFocus, Sarah Granger, *Social Engineering Fundamentals, Part II Combat Strategies*, January 9, 2002
8. Sans Institute 2001, *A Proactive Defense to Social Engineering*
9. TechRepublic, *IT Security Survival Guide, Change you company's culture to combat social engineering attacks. Jason Hiner, 12-15.*
10. Carnegie Mellon University, Software Engineering Institute, CERT Coordination Center; <http://www.cert.org>.

Effective Date: June 2005
Date Last Modified: April 12, 2009