

SOCIAL ENGINEERING - USING HUMAN BEINGS TO CIRCUMVENT SECURITY SURVEY OF THE LITERATURE

*Kanishka Sugathadasa MCSSL, CISA, ACMA
B.Sc. (Hons.) Computer Science – University of London
P.G. Diploma in Business Administration (PIM)
Certified Information Systems Auditor (ISACA)
Former President, Information Systems Audit & Control Association, Sri Lanka Chapter (141)
Managing Director, I.T. Advisors (Private) Limited.*

Abstract: This paper is a literature survey. It introduces the key concepts of Social Engineering. It discusses the types of attacks, and how to become a social engineer and perform social engineering attacks. It then discusses how to identify social engineering attacks, how to deal with them, and how to prevent them.

1. Introduction

Social Engineering “is the hackers clever manipulation of the natural human tendency to trust. The hackers goal is to obtain information that will allow her/him to gain unauthorized access to a valued system and the information residing on the systems” (Sarah Granger).

Traditional technology defences (such as firewalls, Intrusion Detection Systems, systems hardening etc) protects against technology and network attacks, and not against humans, and are totally useless against social engineering. “It’s up to Maggie in accounting or her friend, Will, dialling from a remote site, to keep the corporate network secured” (Sarah Granger).

Technology can be upgraded, but how do upgrade humans? E.G. How do you upgrade a Help Desk operator to fend off a social engineering attack, where hacker poses to be from management and inquires about the unresolved problems from the help desk operator, later to pose as a help desk operator and instruct the user with the unresolved problem to “resolve” the problem by a series of actions which as a by-product installs a spyware program? This is called “Reverse Social Engineering”.

Social Engineering Attacks use Human Nature. Social Engineering employs the default setting in people. As much as the default settings shipped with an operating system, e.g. guest user identities with blank passwords, can be misused, similarly the default trusting nature of human beings can be used to by pass layers of security such as firewalls, encryption etc, by “picking up the phone and just asking for the password”.

Social Engineering uses expert knowledge of human nature (e.g. as detailed by Prof. Cialdini in his book Influence) to trigger automatic behaviour patterns which make us terribly vulnerable to those who know how they work. We have been subject to them from an early point in our lives and have motivated us so pervasively since then that we rarely perceive their power. To do this requires not more than one correctly chosen word that engages a strong psychological principle and sends an automatic behaviour tape rolling within us. Prof. Cialdini likens this to the ancient Japanese close combat technique of Jujitsu where only minimal strength is required to activate forces such as gravity, momentum etc to defeat a far stronger opponent.

2. Target And Attack

Targets are generally larger organisations: telephone companies, answering services, big corporations, financial institutions, hospitals, military and government agencies. However, smaller tech companies (especially after the Internet boom) have been subject to attacks.

Attacks can take place on two levels, physical and psychological. The physical setting could be: the workplace, the phone, your trash, and even on-line.

In the workplace the hacker can walk in to the building and pretend to be a maintenance worker or consultant with access to the organisation. Once access is obtained, the attacker looks for passwords and other information lying around, or watches over the shoulder while an employee types in the password.

The most prevalent type of social engineering is by phone. A hacker will call and imitate someone in positions of authority or relevance and gradually pull information out of the user. Help Desks are particularly vulnerable as they are in place to help. Help desk employees are trained to be friendly and give information and this can be a gold mine for social engineers.

Your trash – called “Dumpster Diving” can yield lot of information for the hacker. The LAN Times listed the following items as potential security leaks:

- Company phone books (names and numbers of persons to target or impersonate),
- Organisational charts (persons in authority in the organisation),
- Memos (give small tidbits of information which aggregate to create authenticity),
- Policy manuals (shows how secure and insecure the company is),
- Calendars of meetings, events and vacations (tells which employees are out of town at a particular time),
- Systems manuals, printouts of sensitive data or login names and passwords, printouts of source code (gives the keys to unlock the systems and network),
- Disks and tapes, and outdated hardware (can be restored to provide information), and
- Company letterheads.

Online social engineering - the Internet is a fertile ground for social engineers to harvest passwords. The first failure is that users use the same password for many accounts. Another to obtain information on-line is to pretend to be a network administrator, and send an email asking for the user's password. Pop-up windows can be installed to look like a part of the network and requests the user to re-enter the user name and password to fix a problem. Email can be used to plant viruses, worms and Trojan horses. Phishing is another technique.

3. Type Of Social Engineering Attacks

We have Active and Passive Attacks.

Passive attack is the gathering of intelligence about the organisation, remembering that people are a more complicated form than reading the manual!

Active attacks elicit a response using the basic human emotions. For example:

- Intimidation – threatening various negative consequences from non-compliance
- Impersonation – classic trick of social engineers
- Blackmail – e.g. emotional blackmail, or even criminal blackmail
- Deception
- Flattery – many people are surprisingly vulnerable
- Befriending – many persons will do for a friend what they will not do for a stranger
- Authority
- Pressure – bad decisions are usually made under pressure
- Vanity
- Sympathy – classic social engineering trick

Combination attacks such as befriending and impersonation can be more effective than a single attack.

The intelligence gathered in the passive stage of the attack will suggest an attacker/target relationship. For example:

ATTACKER / VICTIM POSITION	ROLE PLAYED BY ATTACKER
Attacker in weak position	Helpless victim / In need of help or guidance
Attacker in strong position	Angry boss / Abusive superior
Lateral position	Equal / Friend / Colleague

Some sample attacks using the above model:

Attack 1 – Impersonation

The attacker pretends to be from the cleaning service, e.g. by putting on a uniform of the cleaning service, enters the offices during the evening and gathers passwords etc.

Attack 2 – Impersonation, Lateral Position, and Authority

The attacker claims to be from a hardware vendor supplying equipment to the organisation and telephones the help desk to find out the unresolved problems. He/she then telephones one of the users with the problem claiming to be from the help desk, and outlines a series of actions to be done by the user to resolve the problem which ultimately installs a spyware program in the user's computer.

Attack 3 – Impersonation and Sympathy

The attacker telephones the victim giving the name of a legitimate user and claiming to be the legitimate user and claims the attacker's computer is unavailable due to a virus attack and elicits various confidential information

from the victim. *This has been the basis of the largest computer fraud as recorded in the Guinness Book of Records where the attacker contacted the victim bank, claiming to be from the dealing department of the victim bank, and obtained the day's password on transferring funds by pretending that this password was not available with the attacker due to "the attackers computer being unavailable due to a virus". After which the attacker used the password to transfer money to a Swiss bank account.*

4. How do You Become A Social Engineer And Perform Social Engineering Attacks?

First learn to be comfortable around people and learn to make people comfortable around you. Learn to smile and build *rapport*.

Second, give some thought to your state of mind which should be concentrated and focused. As an example, would you launch a web attack using an out of date broken PC?

Professor Cialdini in his book Influence has outlined *six* methods of influence, namely:

Reciprocation

We may automatically comply with a request when we have been given or promised something of value, such as a gift advice or help. This reciprocation principle exists even when the gift is given without the person receiving asking for the gift.

This is a basic human value that allowed human societies to evolve and is ingrained in us through our genes, since this allows a person to give food, care etc with the expectation that the giving is not wasted as it will be returned in the future.

Examples of attacks:

1. An employee receives a call from the person who identifies himself as being from the IT Department. The caller explains that some company PC's have being infected by a virus not recognised by the anti-virus software, which virus destroys all files. The caller now talks the employee through a series of steps which supposedly removes the virus. Next the caller asks the employee to test a software utility on his/her PC, and the employee reciprocates by complying with the request since the caller has just "prevented" a virus attack.
2. Help a systems administrator and get some help in return.
3. Hold open a door for an employee and see the employee hold open a door for you even to a restricted area.

Consistency

This is the tendency to comply having made a public commitment or endorsement for a cause. Once we have promised something we do not want to appear untrustworthy or undesirable and will tend to follow through in order to be consistent with our statement or promise.

Soliciting the initial commitment is the key.

Example of an attack:

1. The attacker contacts a relatively new employee and informs her of her agreement to abide by security policies. He asks for the password to check that it complies with the security policies. He compliments her on her compliance with the password format requirements of alpha/numeric/length etc and advises her to change her password immediately, since now he (the attacker unknown to the employee) knows the password and should be changed immediately as per company policy. In the meantime the attacker has used the password to log in and plant a Trojan horse program in the employee's computer.

Social Proof

This is the tendency to comply with what the other are doing, so as to, appear in line with what the others are doing. The action of others is accepted as the valid behaviour. Example is after a lecture during the question and answer session where everybody in the audience waits silently until one person to asks a question and suddenly a deluge of questions are asked.

Example of an attack:

1. The caller, who is the attacker, says that he is conducting a survey, and names other people in the Department who have already cooperated with him. The employee, believing that cooperation by others validates the authenticity of the request agrees to take part. The attacker asks a series of questions which allow him to attack the computer system.

Liking

This concept sound trivial but in reality it is nothing of the sort. According to Prof. Cialdini you have to appear similar to the victim you are approaching in beliefs and attitudes. Sometimes a simple compliment will work wonders.

Examples of attacks:

1. The attacker manages to learn a hobby or interest of the victim, and claims an enthusiasm in the same hobby or interest. Or he may claim to be from the same school.
2. Compliment a receptionist to get her cooperation.

Authority

Under pressure from authority people will do things that they will never do on their own. People will comply if they believe that the requestor is person in authority or authorised to make the request.

Examples of attacks:

1. A social engineer claims to be from a hardware vendor and has come to maintain the servers. She gets admission to the main server room.

Scarcity

People perceive what is unavailable as valuable. If you position yourself as unavailable people will flock to you for advice. Just advise them in a manner conducive to your attack.

Example of an attack:

1. Attacker offers free movie tickets to the first 500 to register. To register one must provide his/her email and give a password. There is propensity to reuse passwords. Therefore, the attacker now uses this password to attack home/office computer systems.

These techniques barely scratch the surface of psychological persuasion, and there are even more advanced techniques.

5. Identifying A Social Engineering Attack

Warning Signs of an Attack

- Refusal to give a call-back number
- Out of ordinary request
- Claim of authority
- Stress urgency
- Threatens negative consequences of non-compliance
- Show discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

Common Targets of Attacks:

TARGET TYPE	EXAMPLES
Unaware of Value of Information	Receptionists, telephone operators, administrative assistants, security guards
Possess Special Privileges	Help desk or technical support, systems administrators, computer operators, telephone systems operators
Manufacturer / Vendor	Computer hardware, software manufacturers, voice mail system vendors
Specific Departments	Accounting, human resources

The Social Engineering Cycle:

ACTION	DESCRIPTION
Research	Open source information such as CSE filings, annual reports, marketing brochures, patent applications, press clippings, industry magazines, and Website content. Also, trash cans.
Developing Rapport and trust	Use of insider information, misrepresenting identity, citing those known to the victim, need for help or authority.
Exploiting Trust	Ask for information or an action on part of the victim. In reverse sting, manipulate the victim to ask the attacker for help.
Utilise Information	If the information obtained is only a step to final goal, attacker returns to earlier steps in cycle till goal is reached.

Common Social Engineering Methods:

- Posing as a fellow employee
- Posing as an employee of a vendor, partner company, or law enforcement
- Posing as someone in authority
- Posing as a new employee requesting help
- Posing as a vendor or systems manufacturer calling to offer a systems update or patch
- Offering help if a problem occurs, then making the problem occur, thereby manipulating the victim to call for help
- Sending a free software patch for the victim to install
- Sending a virus or Trojan horse as an email attachment
- Using a false pop-up window asking the user to log on again or sign on with the password
- Capturing the victims key strokes with a program
- Leaving a CD/Floppy around with a malicious software in it
- Using insider lingo or terminology to gain trust
- Offering a prize for registering at a Web site with user name or password
- Dropping a document or file in company mail room for intra-office delivery
- Modifying a fax machine header to make it appear to come from an internal location
- Asking a receptionist to receive and then forward a fax
- Asking a file to be transferred to an apparently internal location
- Getting a voice mailbox setup so that the call-backs perceive the attacker to be internal
- Pretending to be from a remote office and asking for local email access.

Factors which make a company more vulnerable to attacks

- Large number of employees
- Multiple facilities
- Information on employee whereabouts left in voice mail messages
- Phone extensions made readily available
- Lack of security training
- Lack of data classification system
- No incident reporting/response plan

6. Responding To Social Engineering Attacks

When something suspicious is detected, procedures should be in place for tracking the incidents. The Incident Response Team (IRT) should coordinate the response. Others in similar positions should be notified as they also may be subject to the same attack.

7. Preventing A Social Engineering Attack – Begin With Security Policies

Effective countermeasures can be put into place to prevent social engineering attacks. Unless everybody in the organisation understands that security is important and makes it his or her business to know and adhere to security policies, social engineering attacks will pose a grave risk.

Developing suitable policies is the key to preventing social engineering attacks. The policies will comprise: data classification, Verification and authorisation procedures, Management policies, and Information Technology policies. Some of the policies are detailed below.

The following procedures will help to prevent a social engineering attack.

Verification of Identity Procedure

ACTION	DESCRIPTION
Caller Identity	Verify call is internal, and name or extension number matches the identity of the caller
Call Back	Look up the requester in company directory and call back the listed number
Vouching	Ask a trusted employee to vouch for requestor’s identity
Shared Common Secret	Request enterprise-wide shared secret, such as a password or daily code
Supervisor or Manager	Contact employee’s immediate supervisor and request verification of identity and employment status
Secure Email	Request a digitally signed mail
Personal Voice Recognition	For a caller known to employee, validate by caller’s voice
Dynamic Password	Verify against a dynamic password solution such as Secure ID or other strong authentication device
In Person	Require a requestor to appear in person with an employee badge or other identification.

Verification of Employment Status

ACTION	DESCRIPTION
Employee Directory Check	Verify that requestor is listed in on-line directory
Requestor’s Managers Verification	Call requestor’s manager using phone number listed in directory
Requestor’s Department or Workgroup Verification	Call requestor’s department or workgroup and determine that the requestor is still employed by the company

Determining the Need to Know

ACTION	DESCRIPTION
Consult Job Title/ Workgroup/ Responsibilities List	Check published lists of which employees are entitled to specific classified information
Obtain Authority from Manager	Contact your manager, or the manager of the requestor for authority to comply
Obtain Authority from Information Owner or Designee	Ask owner of information if requestor has a need to know
Obtain Authority from Automated Tool	Check proprietary software database for authorised personnel

Verifying Non- Employees

CRITERION	ACTION
Relationship	Verify that the requestor's firm has a vendor, strategic partner or other appropriate relationship
Identity	Verify requestor's identity and employment status at vendor/partner firm
Non-disclosure	Verify that the requestor has a signed non-disclosure agreement on file
Access	Refer the request to management when the information is classified as non-public (see Data Classification below)

Data Classification

CLASSIFICATION	DESCRIPTION	PROCEDURE
Public	Can be freely released to public	No need to verify
Internal	For use within the company	Verify identity of requestor as active employee or verify non-disclosure agreement on file and management approval for non-employees
Private	Information of a personal nature intended for use only within the organisation	Verify the identity of requestor as active employee or non-employee with authorisation. Check with human resources department to disclose private information to authorised employees or external requestors
Confidential	Share only with people with an absolute need to know with the organisation	Verify identity of requestor and need to know from designated information owner. Release only with prior written consent of manager or information owner or designee. Check for non-disclosure agreement on file. Only management personnel may disclose to persons not employed by the company.

8. Preventing Social Engineering Attacks – Physical Attacks

Anyone entering the building should have her identity checked and verified, with *No Exceptions*. Some documents need to be physically locked in file drawers or other safe sites, and the key not be left lying around. Other documents will require shredding. All magnetic media should be bulk erased.

All machines on the network (including remote systems) should be password protected. Screen saver passwords are obligatory. PGP or other encryption programs should protect sensitive data on magnetic media.

9. Preventing Social Engineering Attacks – Phone And PBX

Hackers sometimes call and ask to be transferred to an outside line from which they take expensive overseas or long-distance calls. This can be prevented by disallowing transfers to outside lines, controlling overseas and long-distance calls, and tracing suspicious calls. A phone technician who needs user help to gain access is lying, as phone technicians are trained to conduct test without customer help, and requests for passwords etc should be treated with suspicion.

Help Desks are a major target for social engineering, as they are trained to disclose information helpful to users. Help desks should refuse to give out password without authorisation, and disclosing passwords only in person to trusted, authorised personnel should be a policy. Call backs, PINs and passwords are recommended. Help Desk workers should withhold support for suspicious calls.

10. Preventing Social Engineering Attacks – Training And Re-Training

Training should extend throughout the organisation, at all levels.

Employees must be trained to identify information which should be considered confidential and their responsibility to protect it. Organisations must make computer security a part of the job, even if they do not use computers. SANS organisation recommends a combination of “videos, newsletters, brochures, booklets, signs,

posters, coffee mugs, pens, pencils, printed computer mouse pads, screen savers, logon banners, note pads and desktop artefacts, T-shirts, stickers etc” . These items should be changed regularly.

11. Acknowledgements

This paper is only a literature survey and therefore is based on the following books and articles:

1. Mitnick, Kevin D. *“The Art of Deception”*; Wiley 2002
2. Cialdini, Dr. Robert B. *“The Psychology of Influence”*; Quill William Morrow 1984
3. Peikari, Cyrus and Chuvakin, Anton *“Security Warrior”*; O’Reilly 2004
4. Granger, Sarah *“Social Engineering Fundamentals – Part I Hacker Tactics, Part II – Combat Strategies”*; www.securityfocus.com