SOCIAL ENGINEERING

An attack vector most intricate to tackle!

Abstract

There are several techniques available to a hacker for breaching the Information Security defenses of an organization. The human approach often termed ‘Social Engineering’ and is probably the most difficult one to be dealt with. This paper describes Social Engineering, common techniques used and its impact to the organization. It discusses various forms of Social Engineering, and how they exploit common human behavior. The document highlights ways and means to counter these attacks, and also emphasizes on the importance of policy enforcement and user education in mitigating the risks posed by Social Engineering.

Prepared by:
Ashish Thapar
CISSP # 106841

Introduction

As technical attacks on systems have increased, so have numerous technology based countermeasures being used successfully to thwart them. As a result, attackers are shifting their focus and are increasingly targeting people through the use of social engineering methods, often gaining unnoticed access to computer systems and sensitive data. This is due to the widely accepted fact that People are the ‘weakest links’ in a security framework. In the era of laws and legislations such as SOX (Sarbanes-Oxley), GLBA (Gramm-Leach-Bliley Act), HIPAA (Health Insurance Portability and Accountability Act) and more, it becomes imperative for everyone to prepare, defend and react to these attacks.

What is Social Engineering?

Social Engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or a simple fraud, the term typically applies to trickery for information gathering or computer system access. In most of the cases the attacker never comes face-to-face with the victims and the latter seldom realize that they have been manipulated.

Why Social Engineering?

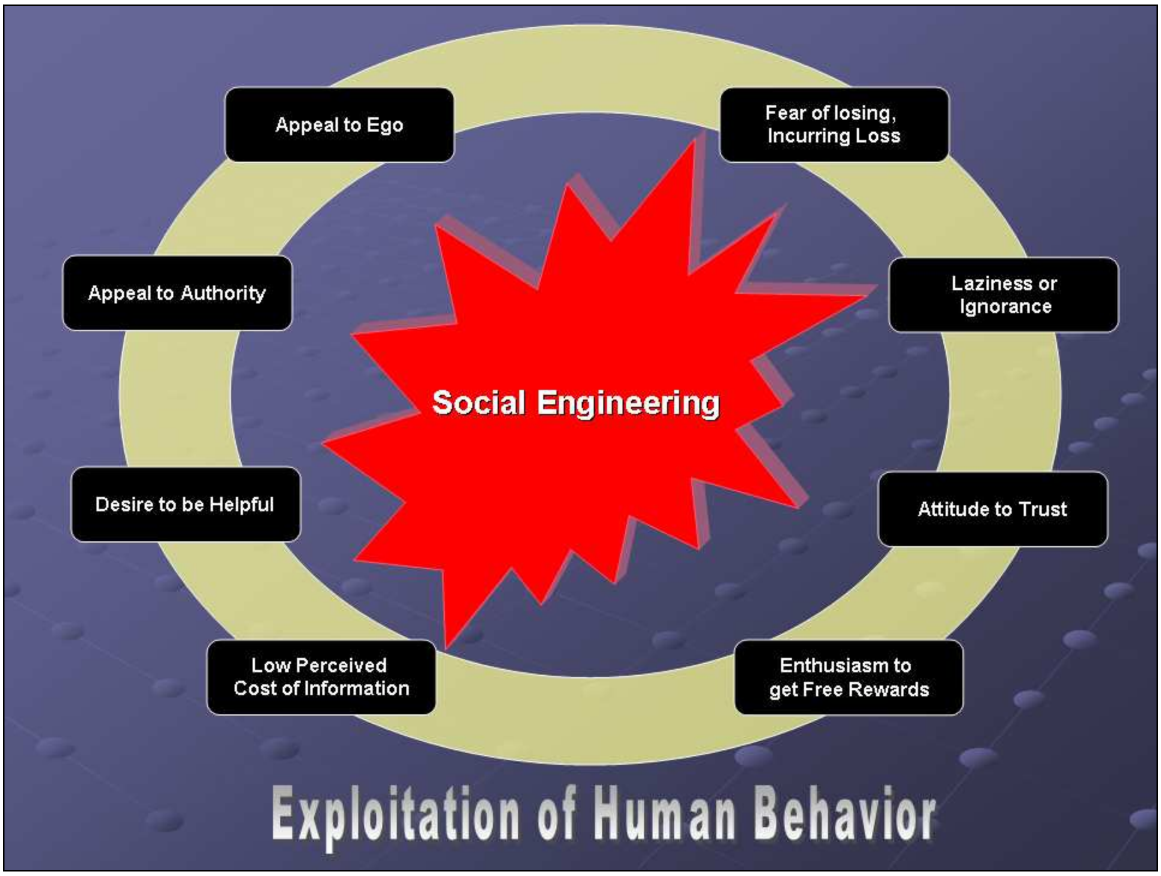
Social Engineering uses human error or weakness (i.e. ‘cognitive biases’) to gain access to any system despite the layers of defensive security controls that may have been implemented. A hacker may have to invest a lot of time & effort in breaking an access control system, but he or she will find it much easier in persuading a person to allow admittance to a secure area or even to disclose confidential information. Despite the automation of machines and networks today, there is no computer system in the world that is not dependent on human operators at one point in time or another. Human interfaces will always be there to provide information and perform maintenance of the system.

Key Challenges

Despite the humungous security threat posed by Social Engineering, very little is ever highlighted about it. Primary reason for the lack of discussion about Social Engineering can be attributed to shame. Most people see Social Engineering as an attack on their intelligence and wit, and no one wants to be considered ignorant or dumb to have been duped. This is why Social Engineering gets hidden in the closet as a "taboo" subject, whereas the fact is that no matter who a person is, he / she may be susceptible to a Social Engineering attack.

Behaviors Vulnerable to Social Engineering Attacks

Social Engineering has always been prevailing in some form or the other; primarily because of the some very natural facets of human behavior. A social engineer exploits these behavior patterns to drive the target towards becoming a victim in the attack. Common human behaviors that are exploited by social engineers are shown in the image provided hereunder.


Appeal to Ego
Fear of losing, Incurring Loss
Appeal to Authority
Laziness or Ignorance
Social Engineering
Desire to be Helpful
Attitude to Trust
Low Perceived Cost of Information
Enthusiasm to get Free Rewards
Exploitation of Human Behavior

Social engineering is still the most effective and probably the easiest method of getting around security obstacles. Sign of a truly successful social engineer is that, they extract information without raising any suspicion as to what they are doing.

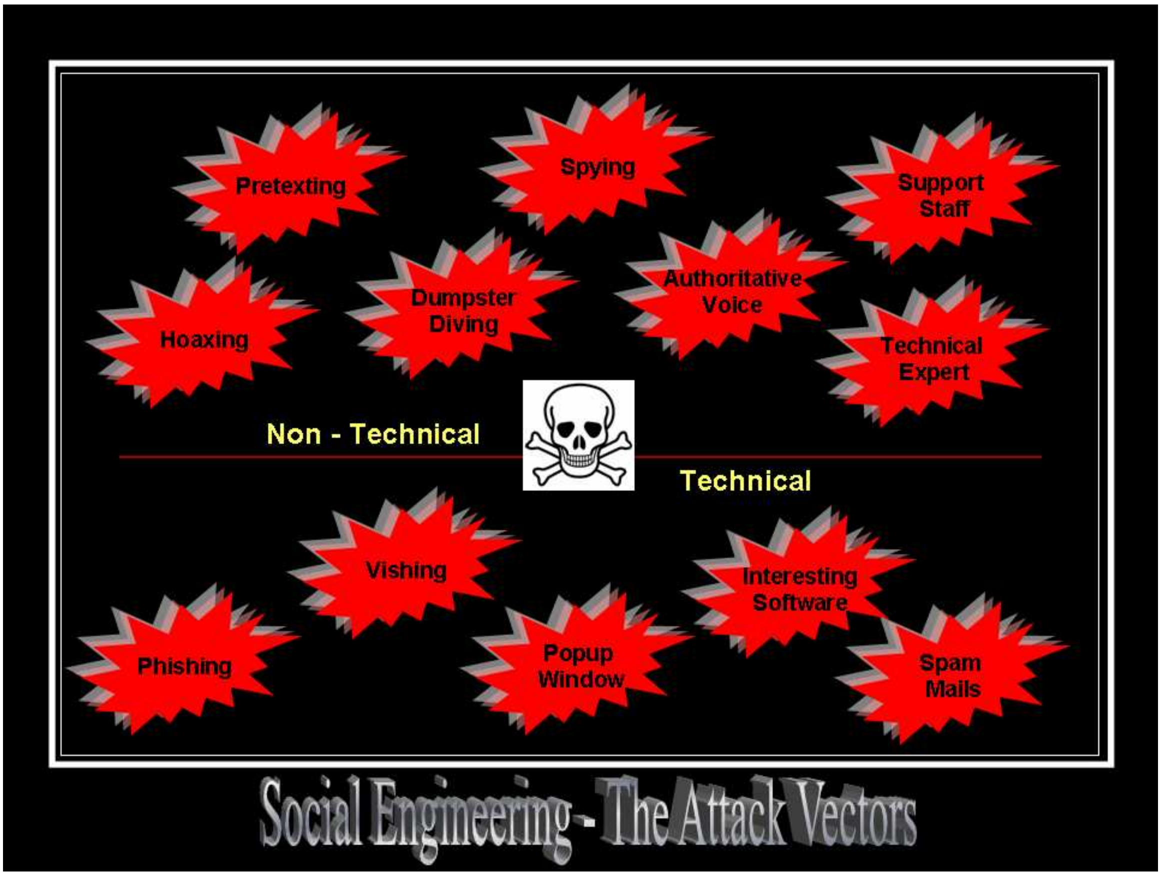
Reverse Social Engineering on the other hand, describes a situation in which the target itself makes the initial approach and offers hacker, the information that they want. Such a scenario may seem unlikely, but figures of authority - particularly technical or social authority - often receive vital personal information, such as user IDs and passwords, because they are above suspicion. In this 'cake-walk' scenario for a hacker, the victims themselves reveal information or provide the access, without someone trying to manipulate them.

Categories of Social Engineering

There are two main categories under which all social engineering attempts could be classified – computer or technology based deception, and purely human based deception.

The *technology-based approach* is to deceive the user into believing that he is interacting with a 'real' application or system and get him to provide confidential information. For instance, the user gets a popup window, informing him that the computer application has a problem, and the user will need to re-authenticate in order to proceed. Once the user provides his ID and password on that pop up window, the damage is done. The hacker who has created the popup now has access to the user's id and password and is in a position to access the network and the computer system with credentials of that user.

Attacks based on *non-technical approach* are perpetrated purely through deception; i.e. by taking advantage of the victim's human behavior weaknesses (as described earlier). For instance, the attacker impersonates a person having a big authority; places a call to the help desk, and pretends to be a senior Manager, and says that he / she has forgotten his password and needs to get it reset right away. The help desk person resets the password and gives the new password to the person waiting at the other end of the phone. The attacker now has all the access to perform any malicious activity with the credentials of actual user.



Technical Attack Vectors

Phishing

This term applies to an email appearing to have come from a legitimate business, a bank, or credit card company requesting "verification" of information and warning of some dire consequences if it is not done. The letter usually contains a link to a fraudulent web page that looks legitimate with company logos and content and has a form that may request username, passwords, card numbers or pin details.

Vishing

It is the practice of leveraging Voice over Internet Protocol (VoIP) technology to trick private personal and financial information from the public for the purpose of financial reward. This term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. However, with the advent of VoIP, telephone services may now terminate in computers, which are far more susceptible to fraudulent attacks than traditional "dumb" telephony endpoints.

Spam Mails

E-mails that offer friendships, diversion, gifts and various free pictures and information take advantage of the anonymity and camaraderie of the Internet to plant malicious code. The employee opens e-mails and attachments through which Trojans, Viruses and Worms and other uninvited programs find their way into systems and networks. He or she is motivated to open the message because it appears to offer useful information, such as security notices or verification of a purchase, promises an entertaining diversion, such as jokes, gossip, cartoons or photographs, give away something for nothing, such as music, videos or software downloads. The outcome can range in severity from nuisance to system slow-down, destruction of entire communication systems or corruption of records.

Popup Window

The attacker’s rogue program generates a pop up window, saying that the application connectivity was dropped due to network problems, and now the user needs to reenter his id and password to continue with his session. The unsuspecting user promptly does as requested, because he wishes to continue working, and forgets about it. Later it is heard that there has been an attack on the system, but it never realized that that he / she was the one who opened the gate!

Interesting Software

In this case the victim is convinced to download and install a very useful program or application which might be ‘window dressed’ as a CPU performance enhancer, a great system utility or as a crack to an expensive software package. In this case a ‘Spyware’ or a ‘Malware’ (such as a key logger) is installed through a malicious program disguised as an interesting message or a legitimate program.

Non-Technical Attack Vectors

Pretexting / Impersonation

This is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone. It's more than a simple lie as it most often involves some prior research or set up and makes use of pieces of known information (e.g. date of birth, mother’s maiden name, billing address etc.) to establish legitimacy in the mind of the target.

Dumpster Diving

Seldom would someone think that throwing away junk mail or a routine company document without shredding could be a risk. However, that is exactly what it could be, if the junk mail contained personal identification information, or credit card offers that a ‘dumpster diver’ could use in carrying out identity theft. The unsuspecting ‘trash thrower’ could give the Dumpster Diver his break. Company phone books, organization charts and locations of employees, especially management level employees who can be impersonated to the hacker’s benefit. Unshredded procedure and policy manuals can help the hacker to become knowledgeable about the company’s policies and procedures, and thus be able to convince the victim about their authenticity. The hacker can use a sheet of paper with the company letterhead to create official looking correspondence. A hacker can retrieve confidential information from the hard disk of a computer as there are numerous ways to retrieve information from disks, even if the user thinks the data has been ‘deleted’ from the disk.

Spying and Eavesdropping

A clever spy can determine the id and password by observing a user typing it in (Shoulder Surfing). All that needs to be done is to be there behind the user and be able to see his fingers on the keyboard. If the policy is for the helpdesk to communicate the password to the user via the phone, then if the hacker can eavesdrop or listen in to the conversation, the password has been compromised. An infrequent computer user may even be in the habit of writing the id and password down, thereby providing the spy with one more avenue to get the information.

Acting as a Technical Expert

This is the case where an intruder pretends to be a support technician working on a network problem requests the user to let him access the workstation and ‘fix’ the problem. The unsuspecting user, especially if not technically savvy, will probably not even ask any questions, or watch while the computer is taken over by the so called ‘technician’. Here the user is trying to be helpful and doing his part in trying to fix a problem in the company’s network.

Support Staff

Here a hacker may pose as a member of a facility support staff and do the trick. A man dressed like the cleaning crew, walks into the work area, carrying cleaning equipment. In the process of appearing to clean your desk area, he can snoop around and get valuable information – such as passwords, or a confidential file that you have forgotten to lock up, or make a phone call impersonating you from your desk. Or take the case of the deceptive telephone repairman. The intruder can pose as a repairman and walk up to your phone and fiddle around with the instrument, and the wiring etc, and in the process spy on your workplace for valuable information that has been left unsecured.

Hoaxing

A *hoax* is an attempt to trick an audience into believing that something false is real. Unlike a fraud or con (which is usually aimed at a single victim and are made for illicit financial or material gain), a hoax is often perpetrated as a practical joke, to cause embarrassment, or to provoke social change by making people aware of something. It also may lead to sudden decisions being taken due to fear of an untoward incident.

Authoritative Voice

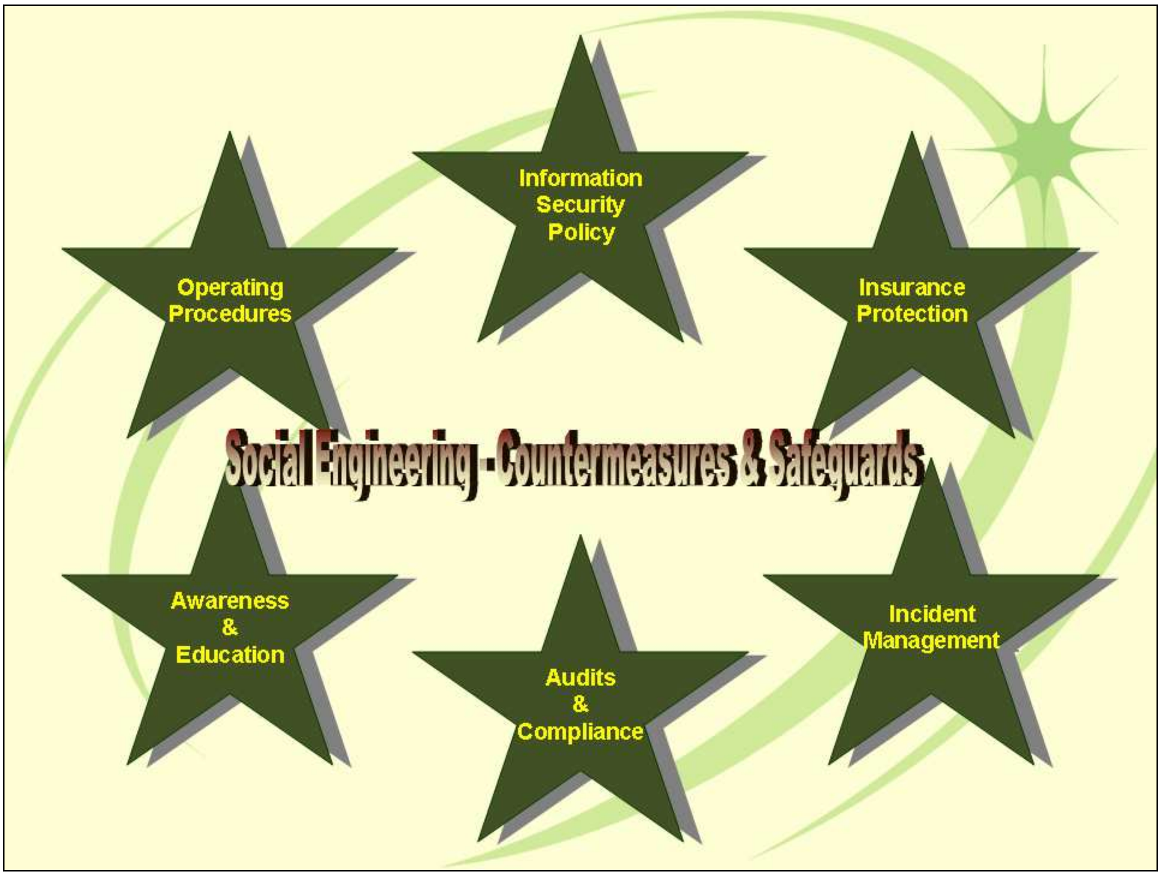
The attacker can call up the company’s computer help desk and pretend to have trouble accessing the system. He / she claims to be in a very big hurry, and needs his password reset immediately and demands to know the password over the phone. If the attacker adds credence to his / her story with information that has been picked up from other social engineering methods, the help desk personnel is all the more likely to believe the story and do as requested.

Impact of Social Engineering on the Organization

Information Security is crucial for any organization as it has become part and parcel of ‘business as usual’ (BAU). If information security is not given priority, especially in the current environment with the variety of threats looming in the environment, even a small lapse in security can bring an organization down. The financial cost could be punitive to the organization and to the individual. There is also the cost of loss of reputation and goodwill, which can erode a company’s base in the long run. For instance, a malicious individual can get access to credit card information that an online vendor obtains from customers. Once the customers find out that their credit information has been compromised, they will not want to do any more business with that vendor, as they would consider that site to be insecure. They could also initiate lawsuits against the company that will lower the reputation of the company and turn away prospective or existing clientele. Over the time, experts have come to the conclusion that despite the impression of the hacker being an outsider wanting to get ‘in’, the majority of violations are caused by either disgruntled employees or non-employees who have legitimate system access because of their job in the organization. In short, companies spend billions of dollars every year in improving hardware and software in order to block malicious attacks. But all of this is an effort in vain if end users are not adequately educated and they good security practices are not being followed.

Countermeasures & Safeguards

Social engineering attacks are one of the hardest threats to defend against because they involve the 'human' element, which in itself is quite unpredictable. Nevertheless, there are some measures which can certainly bring the risk associated with social engineering to acceptable levels. While attacks on human judgment are immune to even the best of security defense systems, companies can mitigate the risk of social engineering with an active security culture throughout the organization that keeps on evolving as the threat landscape changes.



Well Documented Security Policy

A well-documented and accessible Security Policy, associated standards and guidelines form the foundation of a good security strategy. The policy should clearly document in simple terms, its scope and content in each area that it applies to. Along with each policy should be specified, the standards and guidelines to be followed in order to comply with the policy. Generally, a policy should contain policy statements on the domains such as following:

- Acceptable usage policy - for acceptable business usage of email, computer systems, telephone, network etc.
- Information classification and handling – for identifying critical information assets and associated handling instructions

- Personnel security – screening prospective employees, contractors to ensure that they do not pose a security threat to the organization, if employed
- Physical security – to secure the facility from unauthorized physical access with the help of sign in procedures, electronic and biometric security devices etc.
- Information access control – password usage and guidelines for generating secure passwords, access authorization and accountability procedures, securing remote access via modems etc. Automated password reset and synchronization tools can lift the responsibility of managing passwords from tech support and the help desk, without placing an undo burden on end users.
- Protection from viruses – to secure the systems and information from viruses and similar threats
- Information security awareness training – to ensure that employees are kept informed of threats and counter measures and their responsibilities in securing company’s assets
- Compliance monitoring – to continually ensure that the security policy is being complied with.

Risk Assessment

Risk Assessment is a systematic approach that helps management in understanding the risk factors that may adversely affect the organization’s operational capabilities. It also helps in making ‘informed decisions’ about the extent of actions required to mitigate the risk. It involves prioritizing of Information Assets on the basis of risk associated with them. This helps in identification of most critical assets in the organization and focusing organization’s energy and effort in protecting the same. If risk assessment is effectively carried out in an organization, the controls and safety procedures shall protect the most crucial asset against attacks.

Awareness and Education

Building awareness amongst users about the common techniques employed and behaviors targeted by a social engineer is an important part of the defense strategy. Educating employees on the damage done by such theft is also a must. There is no substitute for a good awareness campaign for implementing the ‘social engineering’ elements of a security policy. The elements of an awareness campaign depend on how the information is communicated to staff within the company. The more one reinforces the caution messages within the policies, the more successful is their implementation. The best way to create such awareness in a general non-security professional is through real life examples of companies have been hacked because of insider information, or even just negligence and ignorance on an employee’s part.

Audits and Compliance

Having created the policy and educated the user is not enough, if no one conforms to the policy. Hence there is a need to audit the usage across the enterprise. For example, when a project is going through quality assurance, it should also go through security policy compliance verification. Audit procedures must be in place, to verify for example that the help desk person is not communicating passwords over the phone or via unencrypted email. Periodically Managers should review the access of their employees. Security audits should confirm that employees who no longer need access do not have access. Access points such as entry doors etc should be routinely monitored. This will ensure that employees are complying with policy regarding access to secured locations. Employee workspaces should undergo random inspection to ensure that confidential material is always secured in locked cabinets. Workstations should be locked down and password protected screensavers should be in use.

Identity Management

It is important for organizations to have a unique identifier for each employee. This is often used as their ID to access all computer systems, and also as the key identifier for the individual in the organization. However, keeping the base for personnel identification distinct from that used for computer systems can mitigate this risk. It may lead to some additional work, but it will surely help to limit the damage from an attack.

Operating Procedures

Standard operating procedures, especially those related to providing security access or clearance, should have a cross verification or ‘call back’ step before the request is granted. This will reduce the number of times the hacker can get away with trying to impersonate a legitimate user.

Security Incident Management

When a social engineering attack occurs, make sure that the service desk staff knows how to manage the incident. Each incident provides fresh inputs for an ongoing review of security within the incident response model. To manage an incident, service desk staff must have a robust incident-reporting protocol that records the following information:

- Target name
- Target department
- Date
- Attack vector
- Attack description
- Attack outcome
- Attack effect
- Recommendations

By recording incidents, it is possible to identify patterns and possibly preempt further attacks.

Insurance Protection

Finally, an organization can buy insurance against security attacks. However, most insurers will look for company policies and procedures that work towards reducing the threat of attacks. Generally, insurers are not so much bothered with the security products an organization is using to mitigate attacks as compared to the focus on employee awareness, logical, physical & administrative access controls and security policies put in place.

References:

http://www.microsoft.com/technet/security/midsizebusiness/topics/complianceandpolicies/socialengineeringthreats.mspx

http://en.wikipedia.org/wiki/Social_engineering_%28security%29

http://en.wikipedia.org/wiki/Dumpster_diving

http://www.cisco.com/web/about/security/intelligence/mysdn-social-engineering.html

http://www.windowsecurity.com/articles/Social_Engineers.html

http://www.gartner.com/gc/webletter/security/issue1/article1.html

www.cert-in.org.in