Global Information Assurance Certification Paper

Social Engineering—The Friendly Hacker

Mark Pielocik

GIAC Security Essentials Certification (GSEC)

Practical Assignment Version1.4b

Revision 2.4

Submitted April 29, 2004

Social Engineering (so′sh•l •n′j• nîr ing) *noun* **1.** A non-technical intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.[1] **2.** The act of convincing others to get what you want.[2]

Abstract

Social engineering is, by its nature, a con game used to obtain information that will allow its malicious use to be masked by normal behavior. This paper will examine the types of social engineering, review case studies of how and why information has been compromised, and show how the development of "Information Handling Policies" and "Security Training and Awareness Programs" can help combat social engineering.

Introduction

We have seen security spending consume more and more of our IT budgets over the past several years. Security budgets continued to increase even through the demise of many dotcom companies. This escalating spending on firewalls, intrusion detection, anti-virus, and a myriad of complementary utility tools has focused our awareness on combating attacks based on malicious behavior. This spending on the latest technology has given IT executives a false sense of security.

It's becoming more and more commonplace for IT staff members to be mobilized as a strike team to combat the latest Trojan, worm, or virus. But what about when a person logs into a system with authentic credentials? Does anyone pay any attention? Of course not. Why would we be looking at normal behavior when we're all so focused on abnormal or malicious behavior? Our greatest threat is also our biggest challenge: How do we identify normal behavior with malicious intent?

This paper will use case studies as a means to review potential loss of information as a result of social engineering. In addition, policy development, security training, and awareness programs will be outlined as a means to combat social engineering.

Corporate Culture Evolution

Through the late 90s and into the turn of the century, Corporate America focused on improving customer service. With so many companies providing similar services or selling similar widgets, the best way to distinguish one company from the other was to provide superior customer service. This corporate culture shift has produced a more helpful, friendlier environment where people are willing to

[1] Reference: www.searchsecurity.techtarget.com/
[2] Reference: www.urbandictionary.com

go the extra mile to assist the customer or potential customer. In fact, we have become far too willing to share information.

This author's career took him through numerous training classes and seminars that focused on customer satisfaction, total quality management, and improved communication skills. This good corporate citizen mentality placed an emphasis on being as helpful as possible, regardless of what a person was asking for. Phone etiquette was at the forefront of this training, and we were required to help any caller find at least the correct person or department to assist them in their quest. This corporate culture shift to a more open information flow has provided an environment for social engineering to flourish.

While surfing the web recently, I came across a web site[3] that had a t-shirt for sale. It read, *"Social Engineering Specialist"* on the front and on the back it says, *"Because there is no patch for human stupidity."* Although the statement on the t-shirt was meant as a joke, it makes me think about how easy it is for someone to get information from other people. I don't agree with the statement that there is no patch for human stupidity. I believe you can "patch human behavior" with education and continuous testing. Much like patching a system to get rid of vulnerability, I believe the same concept can be applied to humans through comprehensive education, security awareness, and continuous test programs.

Simon Garfinkal wrote an article[4] in which he states, "The best way to teach employees techniques for resisting social engineering is to repeatedly hit them with mock social engineering attacks." Patches teach computers how to mitigate vulnerabilities and once patched and tested the computers vulnerability has been mitigated. Unfortunately, people tend to forget much of what they learn, so continuous awareness and testing is the best means to mitigate social engineering. Much like the testing procedures we perform after patching a system to see if the vulnerability has been closed, we need to perform continuous testing to ensure our "Social Engineer Patches" are successful.

Types of Social Engineering

I believe social engineering must be broken or segregated into types in order to identify the ways to best mitigate them. The following is a breakdown of the various ways information can be socially engineered and an overview of how each can be mitigated.

[3] Reference: http://www.jinxhackwear.com/scripts/details.asp?affid=-1&productID=122

[4] Reference: October 2002 issue of CSO Magazine; article entitled "Anti-Social Engineering – Lessons From Reading Mitnik."

1. **Human Information Fraud**
   Situation: An employee receives a phone call from a person misrepresenting himself to gain information through deceptive means.

   Mitigations:
   - Train employees not to disclose any information to anyone they do not know.
   - Ensure that employees know what types of information are sensitive and are not to be disclosed.
   - Implement a policy that if someone is looking for information about people in your company, employees are to take their name, company information, and phone number and agree to pass it on to the appropriate parties.

2. **Human Information Mishandled**
   Situation: An employee discloses sensitive information because she is not aware the information is sensitive.

   Mitigation: Implement a comprehensive awareness program to inform personnel of the different categories of information; what is considered sensitive and cannot be disclosed.

   Situation: Employee loses or mishandles identification cards or key/access card.

   Mitigations:
   - Require employees to report lost or stolen identification and key cards. Implement procedures to remove key cards from the systems immediately.
   - Require physical security personnel to check badges for access to a facility.

   Situation: Two employees engage in a conversation regarding sensitive or company-confidential information in inappropriate surroundings; e.g., coworkers discussing the details of a project on a commuter train.

   Mitigation: Review policies and procedures regarding communication of sensitive information on a regular basis.

   Situation: An administrator, super user, or other authorized person shares his passwords with unauthorized personnel.

   Mitigations:
   - Review policies and procedures regarding communication of sensitive information on a regular basis.
   - Perform frequent social engineering tests to see if personnel will divulge their passwords.

3. Physical Information Mishandled

Situation: An employee discards sensitive information where it is readily available for someone to remove from the trash.

Mitigations:

- Review policies and procedures regarding handling of sensitive information on a regular basis.
- Perform frequent searches looking for sensitive information that has been discarded improperly.

Situation: An employee reads sensitive information aloud in a public place where someone could overhear.

Mitigation: Review policies and procedures regarding communication of sensitive information on a regular basis.

Situation: An employee writes down her password and posts it in an easily compromised area; e.g., on a sticky note under her keyboard.

Mitigations:

- Review policies and procedures regarding handling of passwords on a regular basis.
- Create a policy allowing the security team to audit the facilities looking for mishandled passwords.
- Perform frequent searches looking for sensitive information that has been discarded improperly.
- Test the auditors to ensure they are auditing correctly. Use a capture-the-flag process as an incentive to get auditors to really look for mishandled passwords.

Situation: Sensitive or confidential documents are left where they can be casually observed.

Mitigations:

- Review policies and procedures regarding handling of sensitive information on a regular basis.
- Create a policy allowing the security team to audit the facilities looking for mishandled information.
- Perform frequent searches looking for sensitive information that has been discarded improperly.
- Test the auditors to ensure they are auditing correctly. Use a capture-the-flag process as an incentive to get auditors to really look for mishandled passwords.

4. Technological Information Fraud

Situation: An employee receives an e-mail message or URL attempting to trick her into providing company-confidential information.

Mitigations:

- Review policies and procedures regarding handling of sensitive information on a regular basis.
- Create a policy allowing the security team to audit personnel to see if they can be duped into using a fraudulent web site or e-mail.
- Perform frequent audits on personnel to see if they can be duped.

Situation: Key-stroke recorders are used to record user credentials.

Mitigation: Create a policy allowing the security team to audit systems for spy-ware and allow them to perform the audits on a frequent basis.

Case Studies

Here are a few case studies to review how information was socially engineered, the type of social engineering used, and the results or mitigating steps each company took to combat it.

Human Information Fraud – *Company A*

Company A is a widget manufacturing company with several plants across the country. The IT staff is located at the corporate headquarters and performs most of their technical support remotely.

A man who calls himself Joe Admin contacts a remote user on the telephone. He introduces himself as a new system security administrator supporting Company A's UNIX systems and network. He mentions that he works for the IT manager, and that he is part of a new security initiative to harden the systems and network. Joe informs the user that her password has been cracked as part of a routine security audit.

Joe explains the types of characters and length the user's password must be to meet the new minimum security criteria. He recommends that the user review the new security policy's password guidelines section, detailing the systems to which she has access. Joe then asks the user for her password to critique it and point out why it wasn't good enough. The duped user willingly communicates her password to Joe, believing that he is a member of the security team.

Upon closing the conversation, Joe lets the user know that she is not alone—that there are numerous users who don't meet the minimum criteria. He encourages her to pick something a little stronger next time she's prompted to change her password.

This user's account was compromised and, although no sensitive information was contained on the systems she had access to, her account was used to download hacker tools and the systems were used as a jump point for additional hacking.

In this instance, a savvy system administrator noticed an unusual traffic pattern coming from the compromised system and decided to investigate. During the investigation, multiple hidden hacking tools were found. At first it was believed that the user was responsible for this activity and a case was being built to take disciplinary action against her. However, further investigation revealed that the activity occurred during times when the user wasn't working on the system, and it was identified that her account was logging in from a modem connection. The Telecom group identified the phone number where the call was originated. Through a long and arduous process, it was determined that the phone line was an outbound modem connection on a system which had also been compromised from several IP addresses located in Europe.

During the investigation review it was determined that the user didn't follow the security policy guidelines and protect her own password. No information had been lost, so the users' disciplinary action amounted to the proverbial slap on the wrist. However, the end result was the implementation of a security awareness program launched to keep users informed of the current security policies and to audit users' awareness of the security policies.

The audits were successful because they were required in order to receive quarterly bonuses. Employees were required to log onto their Intranet accounts, review the security policies, and take a 5-question multiple-choice quiz in order to receive their checks. The questions were relatively easy and a little common sense would allow them to pass, however the information was critical as a means to measure the effectiveness of the security awareness program, and determine what areas would need the most focus over the next year. In addition, every employee was required to attend an annual security policy review meeting. Changes to security policies were posted on the company's internal web site, and notices were sent to everyone through e-mail, and memos attached to their paychecks.

Company A's Security Awareness Program Outline

- Review security policies with all employees on an annual basis.
- Post updated security policies through e-mail and on the company's internal web site.
- Implement a new, more secure password retention policy, enforcing minimum requirements on length, strength, and password recycling. (Listed below)
- Perform periodic social engineering audits, using both internal and external resources to validate adherence to policy.

- Implement security awareness assessment testing to measure the overall company's security awareness, and target weak areas for improvement.

- Make testing a requirement to obtain annual bonuses.

Company A's Password Policy

1.0 Purpose
This document describes the password requirements and how they should be handled.

2.0 Scope
All Company A personnel with access to any of Company A's computer systems.

3.0 Policy
Password requirements and handling:

1. Passwords minimum length must be 10 characters.
2. Passwords must contain alpha, numerical, and at least one special character, such as @ # $ % ^ & * ( )!.
3. Passwords must not be written down and/or stored in an unsecured area.
4. Passwords are considered property of each individual and disclosure or sharing of passwords for any reason is not acceptable.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
Computers	Systems located in Company A's computer rooms used to support file and print sharing, e-mail, applications, etc. These systems include remote access servers.

6.0 Revision History

Date	Revision	Author
02/02/2003	Draft	Joe Admin

Human Information Mishandled – *Company B*
Company B is a growing financial institute, with 25 offices located in one region of the country. They are looking to expand their operations by acquiring several financial companies in other parts of the country. The IT department has been asked to review the communication, infrastructure, and security of several potential prospects. Company B's IT Security Manager, Pete Security, was given several packets of potential

companies' security profiles. He was asked to estimate how much capital it would take to get each prospective company's security posture to meet Company B's minimum requirements, and to complete it in two days. Pete enlisted the help of two of his security professionals, Jim and Bill. They both thought the schedule was aggressive but agreed it could be done.

Jim and Bill gather all the material and lock themselves in a conference room to review all the prospective companies' security postures. They are making a lot of progress, but there is still a lot of work needed to finish their assessment. Both colleagues are getting hungry, which is causing them to lose their focus. Bill suggests they go to the new trendy restaurant around the corner from the office—it's close and there are some quiet areas perfect for working while they eat. Jim reluctantly agrees.

They finish their dinner and their assessment and leave the restaurant. Bill takes the document, saying that he will review their work on his train ride out of the city. The two part company feeling they have just pulled a rabbit out of a hat. Bill would not have normally taken work like this out of the office; however with such an aggressive deadline, and the fact that he is planning to take tomorrow afternoon off to play golf, he goes against his better judgment.

The train is full because a local sporting event has just ended. Bill begins to review the spreadsheet they produced, entitled "Company B's Prospective Acquisitions—A Security Assessment." Listed in the document are each potential company's name, security equipment, and an estimate of what it would cost to bring them to Company B's minimum security requirements. Bill is so focused on reviewing the document he doesn't notice the person sitting next to him reading it as well. It turns out that his fellow passenger is a manager at a competing financial institute, who brings the news of Company B's potential acquisitions to his management. Company B's competitor undermines their acquisition of these companies and forces Company B to pay more than they should have.

Company B personnel should have followed their security policy regarding the handling of sensitive information.

Company B implemented a security awareness program stressing points on the handling of sensitive information. Every employee was required to addend a yearly training session including taking a test to assess their level of security awareness. 70% was passing grade and employees were required to pass the test. Personnel who had failing grades were required to sit through the security aware program again.

The tests consisted of multiple choice questions and matching policy violation situation to the policies they violated.

Company B's information handling policy

1.0 Purpose
This document describes the handling requirements for sensitive information.

2.0 Scope
All Company B personnel responsible for working with sensitive information are required to follow this policy.

3.0 Policy
Sensitive information handling policy:

1. All information categorized as sensitive must be secured at all times.
2. Sensitive information must not be shared with internal personnel who are not authorized to view it.
3. Sensitive information must not be shared with external entities unless a nondisclosure agreement has been signed by the entity.
4. Sensitive information must not be removed from Company B's facilities without authorization.
5. Sensitive information authorized to leave Company B's facilities must be secured and is the sole responsibility of the Company B's employee who has the authorization.
6. Sensitive information authorized to be sent to an external entity must use secure transactions to transfer the information.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
Sensitive Information	Any information that is categorized as sensitive. This includes customer, business partner, personnel, and financial data.
Secure Transaction	Any form of secure communication used for the purpose of business transactions. This includes VPN secured e-mail communications, SSL-enabled web transactions, and PGP encrypted messages.
External Entity	Any company that provides goods or services to Company C, and requires a financial transaction as a result of these goods or services. These include hardware, software, and consulting vendors

6.0 Revision History

Date	Revision	Author
4/02/2001	Draft	Pete Security
4/12/2002	Rev 1.01	Pete Security
4/20/2003	Rev 1.02	Pete Security

Technological Information Fraud – *Company C*

Company C is an advertising company with offices in 27 metropolitan areas.

A network professional, we'll call Sarah Network, from Company C receives an e-mail alert from an on-line auction site stating that their accounts have been compromised. The e-mail instructs recipients to change their passwords immediately, and provides a link to a web site where account credentials can be changed.

Sarah clicks on the URL which promptly displays a form to change her information. The site appears to be legitimate, incorporating the company logo and formatting identical to that of the on-line auction site. Sarah, being very security-conscious, immediately complies with the request and enters her current and new user credentials in order to change them. Upon clicking the Submit key she notices the information being posted to an IP address rather than the company's URL. This arouses her suspicions, so she opens a new browser window, types in the auction site's URL, and attempts to log in using her new credentials. Sarah is unable to log into her account. She tries again using her original account information and is authenticated. Sarah immediately changes her user name and password, and contacts the auction site's help desk to ask about the e-mail notification. It turns out the auction company hadn't sent the e-mail, but were aware of the fraudulent attempts to steal members' credentials.

This would have been a disaster if it wasn't for Sarah's suspicious nature. Since her account wasn't used frequently, several fraudulent transactions could have taken place before Sarah would have become aware of the situation. When it comes to security and the possibility of an account being compromised prompt, prudent judgment is required.

The end result was that Sarah wrote two security policies for her company. The first was the "External Entity Communication Handling Security Policy" for e-mail communication with external entities, and the second was the "External Account Security Policy" for the purpose of securing external accounts. These policies are listed below.

Company C's Audit and awareness program outline

- Implement quarterly reviews of the security policies at a departmental level.
- Require that ten percent of every employee's performance assessment is based on their security awareness.

- Update and post security policy internal web site.
- Contract a third party to periodically audit social engineering and use the results to target the groups that need additional training.

Company C's External Entity Communication Policy

1.0 Purpose
This document describes the communication protocol required when exchanging information with external entities.

2.0 Scope
All Company C personnel responsible for business-to-business communication are required to adhere with this External Entity Communication Handling Security Policy.

3.0 Policy
Communication with External Entities will be handled using the following Policy:

1. Communication with external entities with intent to exchange non-sensitive information can utilize the following methods: phone, fax, HTTP, and clear text e-mail.
2. Communication with external entities with intent to exchange sensitive information can utilize the following methods: phone, fax, HTTPS, and encrypted e-mail (PGP Encryption is preferred).
3. All sensitive communication requests from external entities must be validated by the external entity's point of contact.
4. All sensitive communications will utilize secure transactions.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
External Entity	Any company that provides goods or services to Company C, and requires financial transaction as a result of these goods or services. These include hardware, software, and consulting vendors.
Secure Transaction	Any form of secure communication used for the purpose of business transactions. These include VPN secured e-mail communications, SSL-enabled web transactions, and PGP encrypted messages.
External Entity	Any company that provides goods or services to Company C, and requires financial a transaction as a

result of these goods or services. These include hardware, software, and consulting vendors.

6.0 Revision History

Date	Revision	Author
12/02/2003	Draft	Sarah Network
12/12/2003	Rev 1.01	Sarah Network
12/20/2003	Rev 1.02	Sarah Network

Company C's External Account Security Policy

1.0 Purpose

This document describes security requirements for handling External Accounts.

2.0 Scope

All Company Cs' personnel responsible for logging into external accounts for the purpose of Business to Business relations, will adhere to the security policy listed in this document. Failure to comply with this policy will be met with disciplinary action and possible termination.

3.0 Policy

External Accounts for the purpose of Business to Business relations will be setup through the Purchasing Departments Vendor Approval process including the signing of a Non-disclosure agreement with the external Company. The Following information deals with the handling and security of the Approved Vendors External Account.

Account Setup

5. Initial Account Setup will be requested by the individual authorized to perform transactions with the external entity. Once approved by the Purchasing department approval process the account request will be submitted to the external entity.
6. The account credentials setup by the external entity will be sent to the individuals using secure communication.
7. The approved individual will then log into his or her account and change the password.
8. This account and password information must not be written down in an un-secure location.
9. This account information must not be shared with any individual and security of the account is the sole responsibility of the requester.
10. The password for this account must be changed on a quarterly basis.
11. The password for this account must never be re-used.

12. The password for this account should be generated using a "random password generation" utility like Atoy's password generator 1.2 [5]

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
Random password generation	this is a tool that will generate password using numbers, letters and special characters to create a password that is difficult to crack.

6.0 Revision History

Date:	Revision	Author
12/03/2003	Draft	Sara Network

Physical Information Mishandled – *Company D*

Company D is a large service provider, providing Internet and communications services to hundreds of companies including some very large financial institutes. The IT department is comprised of highly trained professionals, and the company's reputation is one of the best in the industry.

Company D's facilities are very impressive and they often take prospective customers on tours. During one such tour, a prospective customer's security manager wanders into an unoccupied cubicle to admire some of the detailed network schematics displayed on the wall. The customer is amazed at the quality and detail of these schematics. He is also amazed to see that most of the drawings are labeled "confidential," and that they are displayed in the open for anyone to view. He notes several company names on the documents and when they return to a conference room to discuss Company D's security profile; he asks if it is common practice to leave confidential documentation displayed on cubicle walls. Company D's CSO, surprised by the comment, proceeds to run damage control and assure the potential customer that none of this information would ever fall into the wrong hands. He also states that they screen every employee and perform background checks on everyone. He explains that the area they toured is very secure, and that only authorized personnel are allowed. He also adds that based on their conversation he would create a security

[5] http://www.atory.com/Password_Generator/

policy that would prohibit confidential information from being displayed or left in the open to be causally observed.

After the meeting, Company D's security group creates two policies, which are listed below. These policies provide the guide lines for handling confidential information and gave the security team the authority to perform random audits of the office area looking mishandled confidential information.

Company D's Confidential Information Policy.

1.0 Purpose
This document describes the required handling of confidential information.

2.0 Scope
All Company D personnel responsible for working with confidential information are required to follow this policy.

3.0 Policy
Confidential information handling policy:

1. All information categorized as confidential must be secured at all times.
2. Confidential information must not be shared with any unauthorized internal personnel.
3. Confidential information must not be displayed or be left in visible to casual observers.
4. Confidential information must be shredded prior to being discarded.
5. Confidential information cannot be shared with any external entity unless there is a valid, signed a nondisclosure agreement and they have been authorized by the Security Department.
6. Exchange of this information must utilize secure transactions.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
Confidential Information	Information containing customer-specific information or information containing Company D-specific information.
Secure Transaction	Any form of secure communication used for the purpose of business transactions. This includes VPN secured e-mail communications, SSL-enabled web transactions, and PGP encrypted messages.

6.0 Revision History

Date	Revision	Author
4/02/2001	Rev 1.01	Dave Security

Company D's Audit Policy

1.0 Purpose
This document describes the audit process for confidential information.

2.0 Scope
All Company D security personnel are authorized to perform physical audits of confidential information.

3.0 Policy
Audit for confidential or sensitive information:

1. This policy authorizes Company D's security personnel access to all areas including office areas, data centers, and service facilities with out notice.
2. Security personnel are authorized to search all areas for confidential information that has not been properly secured. This includes checking that file cabinets have been lock.
3. Security personnel are authorized to look for passwords that have been written down and have not been secured.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	Definitions
Confidential Information	Information containing customer-specific information or information containing Company D-specific information.

6.0 Revision History

Date	Revision	Author
8/02/2003	Draft	Dave Security

Conclusion
Since we have a tendency to forget what we've learned and bad habits have a way of creeping back into our lives, it is my belief that the best way to combat "social engineering" is through continuous security awareness training and auditing process. This awareness process must make us conscious of what information can and can't be disclosed, how to handle this information and the methods to audit ourselves. Continuous and repetitive use of this methodology will lead to a "Socially Secure" security posture.

List of References

[1] www.searchsecurity.techtarget.com/

[2] www.urbandictionary.com

[3] http://www.jinxhackwear.com/scripts/details.asp?affid=-1&productID=122

[4] October 2002 issue of CSO Magazine; article entitled “Anti-Social Engineering – Lessons From Reading Mitnik.”

[5] http://www.atory.com/Password_Generator/