Social Engineering

Security Awareness Series

Cucu Sukmana

Social Engineering- Fact or Fallacy?

From Nov. 12, 2001 Fortune Magazine
"Ask Annie" Column

Dear Annie,
I compile market research , including information about our competitors, for a small software company. Most of it comes from the WEB, news articles, legitimate industry contacts, or industry reports we purchase. Now my boss wants me to start calling our largest competitors, posing as a potential reseller, to try to get product information out of them that way. I don't feel this is ethical. Am I just being a Pollyanna? Does everyone do this?

- *Squeamish in Seattle*

Objective

At the conclusion of this session,

Attendees should be better able to:

Understand the principles of social engineering

Define the goals of social engineering

Recognize the signs of social engineering

Identify ways to protect yourself from social engineering

Agenda

Introduction and Example

Social Interaction influences of social engineering Principles

- Different avenues of persuasion
- Perception

Common types of social engineering

- Human-based
- Computer-based

Agenda

Personality Traits

- Diffusion of responsibility
- Chance for ingratiation
- Trust relationship
- Moral duty
- Guilt
- Identification
- Desire to be Helpful
- Cooperation

Agenda

Social Engineer Exploits

- Direst request
- Contrived situation
- Personal persuasion

Potential Security Breaches

- Passwords
- Modems
- Help Desk
- Websites

Agenda

Employee Education

Recognize the Signs

How to Protect Ourselves

Summary

Case Study Review

Social engineering

Social engineering is the name given to a category of security attacks in which someone manipulates others into revealing information that can be used to steal, data, access to systems, access to cellular phones, money or even your own identity. Such attacks can be very simple or very complex. Gaining access to information over the phone or through web sites that you visit have added a new dimension to the role of the social engineer.

Social engineer

Social Engineering is the acquisition of sensitive information or inappropriate access privileges by an outsider, based upon the building of an inappropriate trust relationship with insiders.

The goal of social engineering is to trick someone into providing valuable information or access to that information.

Social Engineering Example

Mr. Smith: Hello?

Caller: Hello, Mr. Smith. This is Fred Jones in tech support. Due to some disk space constraints, we're going to be moving some user's home directories to another disk at 8:00 this evening. Your account will be part of this move, and will be unavailable temporarily.

Mr. Smith: Uh, okay. I'll be home by then, anyway.

Caller: Good. Be sure to log off before you leave. I just need to check a couple of things. What was your username again, smith?

Mr. Smith: Yes. It's smith. None of my files will be lost in the move, will they?

Caller: No sir. But I'll check your account just to make sure. What was the password on that account, so I can get in to check your files?

Mr. Smith: My password is tuesday, in lower case letters.

Caller: Okay, Mr. Smith, thank you for your help. I'll make sure to check you account and verify all the files are there.

Mr. Smith: Thank you. Bye.

Introduction

Social engineering preys on qualities of human nature:

the desire to be helpful

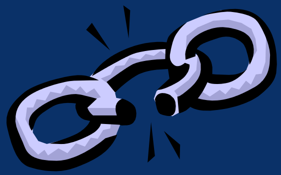
the tendency to trust people

the fear of getting into trouble

The sign of a truly successful social engineer is they receive information without raising any suspicion as to what they are doing.

Introduction

People are usually the weakest link in the security chain.



Social engineering is still the most effective method getting around security obstacles.

A skilled social engineer will often try to exploit this weakness before spending time and effort on other methods to crack passwords.

Introduction

Why try to hack through someone's security system when you can get a user to open the door for you?

Social engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone.

A successful defense depends on having good policies in place ensuring that all employees follow them.

Influences of Social Engineering

Three aspects of social interactions will help us in finding ways to learn about and detect social engineering.

Different avenues of persuasion

Perception that affect social interaction

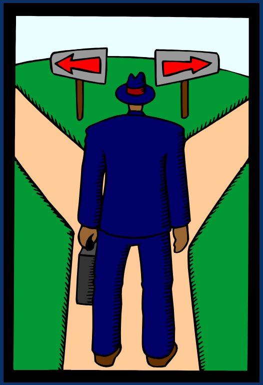
Techniques for persuasion and influence.

Different avenues of persuasion

In attempting to persuade someone to do something, there are two methods a persuader can employ:

A Direct Route

A Peripheral Route



Different avenues of persuasion

A Direct Route uses:

systematic

logical arguments

To:

stimulate a favorable response

prompting the recipient to action

Different avenues of persuasion

A Peripheral Route uses:

peripheral cues

mental shortcuts

Misrepresent their objectives

To:

trigger acceptance without thinking

Different avenues of persuasion

One way in which the social engineer can make prospective victims more susceptible to Peripheral routes to persuasion is by making some statement at the outset that triggers a strong emotion such as:

Excitement

Fear

“The President of the University is waiting for the information!”

Perception

In a typical transaction our perceptions about the request for service begins with a basic belief that each party is who they say they are.

Some social engineering victims may tend to rely primarily on their belief that the person with whom they dealt was honest, and to give little thought to the activities.

Common Types of Social Engineering

Social engineering can be broken into :

Human based

Computer based

Human-based refers to person-to-person interactions to retrieve the desired information.

Computer-based refers to having computer software that attempts to retrieve the desired information.

Human-based

Impersonation - Case studies indicate that help desks are the most frequent targets of social engineering attacks.

– A Social Engineer calls the help desk

– Help desk is helpful

– Social engineer will often know names of employees

Important User - A common ploy is to pretend be not only an employee, but a vice president.

– Help desk is less likely to turn down a request coming from a high-level official

– Social engineer may threaten to report the employee to their supervisor.

Human-based

Third-party Authorization - The social engineer may have obtained the name of someone in the organization who has the authority to grant access to information.

– Ms. Martinez says its OK.

– “Before he went on vacation, Ms. Martinez said I should call you to get this information.

Tech Support - Social engineer pretends to be someone from the infrastructure-support groups.

– System is having a problem

– Needs them to log on to test the connection

Human Based

In Person - The social engineer may enter the building and pretend to be an employee, guest or service personnel.

– May be dressed in a uniform

– Allowed to roam

– Become part of the cleaning crew

Dumpster diving - Going through the trash

Shoulder Surfing - Looking over a shoulder to see what they are typing.

– Passwords

– Phone-card numbers

Computer-based

Popup Windows - A window will appear on the screen telling the user he has lost his network connection and needs to reenter their user name and password.

- A program will then e-mail the intruder with the information.

Mail attachments - Programs can be hidden in e-mail attachments.

- Viruses
- Worms
- "I love you"

Computer-based

Spam, Chain Letters and Hoaxes **-** These all rely on social engineering to be spread.

– While they do not usually cause damage, they do cause a loss of productivity.

– They use valuable network resources.

Websites **-** A common ploy is to offer something free or a chance to win a sweepstakes on a Website.

– To win requires an e-mail address and password.

– Used with 401K come-on.

Personality Traits

In the following discussion we will examine how various social engineering personality traits enhance the possibility of successful social engineering.

When present, these traits increase the likelihood of compliance.

Personality Traits

Diffusion of responsibility - The target is made to believe that they are not solely responsible for their actions.

– The social engineer creates situations with many factors that dilute personal responsibility for decision making.

– The social engineer may drop names

– May claim someone higher up has made the decision

Chance for ingratiation - The target is lead to believe That compliance with the request will enhance their chances of receiving benefit.

– Gaining advantage over a competitor

– getting in good with management

– Giving assistance to a sultry sounding female

Personality Traits

Trust Relationships - The social engineer expends time developing a trust relationship with the intended victim.

– Usually following a series of small interactions

Moral duty - Encouraging the target to act out of a sense of moral duty or moral outrage.

– Requires the social engineer to gather information on the target and the organization

– Tries to get the target to believe that there will be a wrong that compliance will mitigate

Personality Traits

Guilt - Most individuals attempt to avoid the guilt feelings if possible.

– Social engineer create situations designed to:

· tug at the heartstrings

· manipulate empathy

· create sympathy

– If granting a request will lead to avoidance of guilt, target is more likely to comply.

– Believing that not granting the request will lead to significant problems to the requestor is often enough to weigh the balance in favor of compliance with the request.

Personality Traits

Identification - Try to get the target to identify with the social engineer.

– The social engineer tries to build a connection with the target based on information gathered.

– Informality is another trait social engineers excel at

Desire to help - Social engineers rely on people’s desire to be helpful.

– Holding the door

– Logging on to an account

– Lack of assertiveness or refusal skills

Personality Traits

Cooperation - The less conflict with the target the better.

– Voice of reason

– logic

– patience

– Stresses the positive but can refer back to the threat process

Social Engineer Exploits

Social engineering exploits often fall into one of the following categories:

Direct requests - the social engineer simply asks for the information or access with no set up.

- These are often challenged and refused
- Is seldom used due to low probability of success

Social Engineer Exploits

Contrived situation - The more factors the target must consider in addition to the basic request, the more likely the target is to be persuaded.

– Forgot a password

– manager on vacation

– looming deadlines

Personal Persuasion - Many social engineers are adept at using personal persuasion to overcome initial resistance.

– The goal is not to force compliance but to get voluntary action

– Target believes they are making the decision

Potential Security Breaches

Some potential security breaches are so mundane that they hardly seem noticeable. With the rush to install the latest and greatest firewalls, encryption software and keys, security professionals often overlook the most obvious factors.

Potential Security Breaches

Passwords - One of the weakest areas of security.

– Too long

– Too short

– Too easy

– Never changed

Potential Security Breaches

Modems - Every company has more modems than they know of.

– Programs like *pcAnywhere*

– Use war-dialers

Help Desk - They try too hard to be helpful.

Websites - As we discussed before, setting up a bogus website to trap information.

Common Defenses

A social engineer may simply walk in and behave like one of the employees.

We don’t challenge unfamiliar personnel.

Common Defenses

Common defenses:

- Everyone that enters the building (contractors, business partners, vendors, employees)must show identification
- Passwords are never spoken over the phone.
- Passwords are not to be left lying around.
- Caller ID technology.
- Invest in shredders.

Policies and Procedures

Security policies should cover the following areas:

- Account setup
- Password change policy
- Help desk procedures
- Access privileges
- Violations
- Unique user identification

- Confidential information handling
- Modem usage and acquisition
- Secure sensitive areas
- Privacy policy
- Centralized security focus point

Recognize the Signs

Recognize key signs that indicate you may be the target of a social engineering attack:

Refusal to give contact information

Rushing

Name-dropping

Intimidation

Small mistakes

Requesting forbidden information

Recognize the Signs

“I cannot be contacted”

“I’m on my cell phone and the battery is about to die”

The number they give you is a “call out only” number.

How to Protect Ourselves

Here are some methods:

Become familiar with the techniques used

Trust your instincts

Notification to targeted groups during attempts

Coordinated response when scams are identified

Test your readiness

How to Protect Ourselves

Apply technology where you can.

Consider the following:

- Trace calls if possible
- Control overseas long distance service to most phones
- Ensure good physical security for building access
- Mark sensitive documents

Summary – Four Step Plan

Step 1

If you cannot personally identify a caller who asks for Personal information about you or anyone else (including badge number or employee number), for information about your computer system, or for any other sensitive information, do not provide the information. Insist on verifying the caller’s identity by calling them back at their proper telephone number as listed in (Company Name)’s telephone directory. This procedure creates minimal inconvenience to legitimate activity when compared with the scope of potential losses.

Step 2

Remember that passwords are sensitive. A password for your personal account should be known ONLY to you. Systems administrators or maintenance technicians who need to do something to your account will not require your password. They have their own password with system privileges that will allow them to work on your account without the need for you to reveal you password. If a system administrator or maintenance technician asks you for your password, be suspicious.

Step 3

Systems maintenance technicians from outside vendors who come on site should be accompanied by the local site administrator (who should be known to you). If the site administrator is not familiar to you, or if the technician comes alone, it is wise to give a call to your known site administrator to check if the technician should be there.

Unfortunately, many people are reluctant to do this because it makes them look paranoid, and it is embarrassing to show that they do not trust a visitor.

Step 4

If you feel you have thwarted or perhaps been victimized by an attempt at social engineering, report the incident to your manager and to security personnel immediately.

Final Thoughts

A social engineer with enough time, patience and tenacity will eventually exploit some weakness in the security of an enterprise.

The University's campus constituents awareness and acceptance of security policies and procedures are an important asset in the battle against attackers.

The best defense against social engineering attacks combines raising the bar of awareness among students, faculty and staff, coupled with a sense Of personal responsibility to protect the University's assets.

Final Thoughts

Consequences of successful attacks:

loss of public confidence

market share

negative publicity

fines and other regulatory consequences

Final Thoughts

The audio is NOT true!

Employees at all levels need to believe that they are an important part of the overall security strategy designed to protect the University, its assets, and all those that work and live on campus from the negative consequences of social engineering.

SEC-U-R-IT-Y

Social engineering Case Studies

How would you respond?

Using Names

"Hello, can I speak with Tom Smith from
R&D please?"
"I'm sorry, he'll be on vacation until next Monday"
"OK, who's in charge until he gets back?"
"Robert Jones"

So we speak to Robert Jones instead. A hacker, however, can leverage this information when contacting R&D later. After some small talk with an R&D employee, the hacker claims:

"By the way Michael, just before Tom Smith went on vacation, he asked me to review the new design. I talked with Robert Jones and he said you should just fax/mail/send it to me. My number is 123-1234. Could you do it as soon as possible? Thanks."

Vendor Impersonation

Another basic technique is impersonating an employee from a hardware vendor. They might use the name of a real or imagined company:

"Hi, I'm calling from Applied Technology Corporation. We have a special offer on routers. Could you tell me if you're satisfied with the hardware you're using at the moment?"

After Hours

During an after hours Internet chat session, you are asked for a picture of yourself. Although you don’t have one available, you are obligingly asked if you would like one of the other party. After a bit of additional encouragement, the other party sends An attachment that, in all respects, resembled a JPEG file. Upon accessing the attachment the hard drive starts spinning, and of course, there is no photo.

Understand the danger of a Trojan horse being enclosed, and immediately alert the IT department. The Internet connection needs to be closed down and checked. Eventually, the computer could be reinstalled and rolled back to the day before with a backup tape, (losing a full day of production and possible additional days overall).