Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 12
SOCIAL ENGINEERING

DRAFT

HACKING IS LEARNING
www.hackerhighschool.org

ISECOM

WARNING

The Hacker Highschool Project is a learning tool and as with any learning tool there are dangers. Some lessons, if abused, may result in physical injury. Some additional dangers may also exist where there is not enough research on possible effects of emanations from particular technologies. Students using these lessons should be supervised yet encouraged to learn, try, and do. However ISECOM cannot accept responsibility for how any information herein is abused.

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool Project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license, including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the HHS web page at http://www.hackerhighschool.org/licensing.html.

The Hacker Highschool Project Project is an open community effort and if you find value in this project, we ask that you support us through the purchase of a license, a donation, or sponsorship.

Table of Contents

Contributors

Marta Barceló, ISECOM

Pete Herzog, ISECOM

Bob Monroe, ISECOM

Steve Watts

Greg Playle

ISECOM

Introduction and Objectives

In previous lessons, you've been introduced to the concepts of hacking, and these concepts have usually centered on hacking a computer like a Windows or Linux machine.

Social Engineering (SE), however, isn't a technical skill, though it is seen as the skill of hacking the human; compromising the most complex computer on the planet...the human brain!

There are numerous definitions of SE but for the purpose of this lesson we've defined it as follows **"convincing someone to do something for you that will ultimately lead you to achieve your desired goal, usually without them realizing it."** In the context of Hacker Highschool our aim is usually to circumvent a security control.

This lesson will cover the following:

- Who uses SE and why?
- Information Gathering and Profiling
- Pretexting
- SE Tools
- Protecting against Social Engineers

Along the way we'll give you real life examples of social engineering and how it is used as well as providing you with exercises to allow you to practice and refine your newly found skills. Once you know these skills, you will know what to look for to avoid being "engineered".

Why use Social Engineering rather than hacking?

Passwords, firewalls, security policies, security doors, man traps, biometric scanners, security guards...all of these security controls are useless against a skilled social engineer (also abbreviated SE). Why? Because social engineers prey on the weakest link in the security chain – the human!

SE requires a completely different set of skills than any type of hacking you may have ever done. As a SE, you must be convincing, able to think quickly, look the part you are playing, know your target well enough to move around their environment without acting suspicious, and you must be able to control your own fears. There are very few successful SEs that are also successful hackers. SEs tend to be outgoing and have personalities that attract other people. Hackers tend to have poor social skills and enjoy spending time by themselves. Hackers do their best work when everyone else is asleep and you are alone with your tools.

Society has trained most people to be polite, be obedient, help others, avoid conflict and also to trust and believe what they are told. It is these inherent, natural vulnerabilities that the social engineer aims to exploit by upsetting the balance between common sense and psychological programming and conditioning (see below).

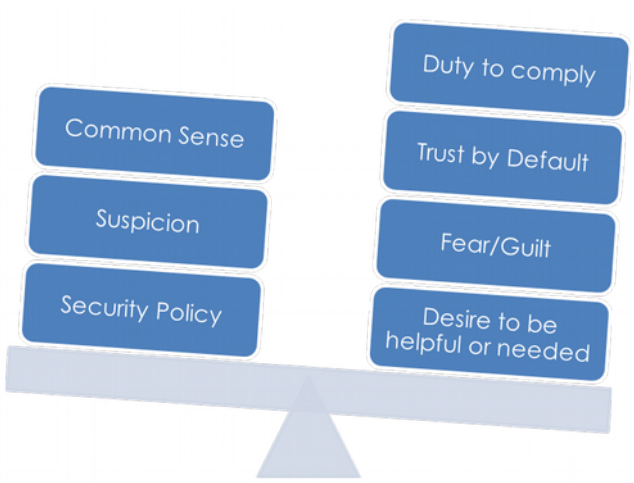


Figure 1: Upsetting the balance

The theory of social engineering is that going after securities weakest link (the human) is far easier than trying to compromise a series of in-depth defensive technical solutions that a company may have in place. Computers do exactly what they are programmed to do; people do not. Humans have emotions, insecurities, desires, and need to fit into society. Computers do not care about promotions or holding the door open for someone with their arms full, or smiling when introduced to a new user. From the time we are raised, our parents teach us to respect our elders, wait your turn to speak, be a good host, tuck your shirt in and so forth. Automation doesn't have manners.

Any psychology book will show you the very basic human needs to fit into society. Face it, we don't want to go around making other people mad at us. We all want to express ourselves as individuals but we don't want to become outcasts. Suppose you meet someone in the mall: If the other person is cute and gives you a friendly smile, it's guaranteed that you will trip over yourself to get more attention from this stranger. Don't deny it. It happens to everyone except Wall Street Brokers and English teachers, for some odd reason.

In Figure 2 below, you can see it is much easier for a SE to compromise the human to get to what they want instead of going through countless other security measures.

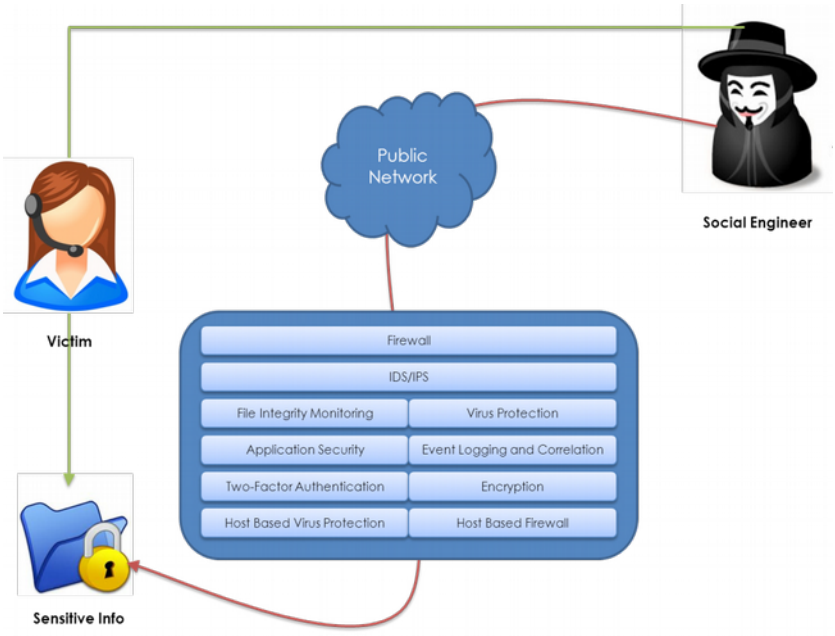


Figure 2: The weakest link in the chain

A SE will employ various psychological techniques including deceit, manipulation, guilt and fear in order to get a victim to do what he wants.

> **Example:** An employee at VictimCo has just used their swipe card to open the door to their secure building when they hear "Hey, excuse me: Could you hold the door, please?" The employee turns around and someone is approaching with a tray full of coffee cups and a phone held to their ear. As they approach the employee hears the person talking into the mobile phone say that he's working on VictimCo's latest product but popped out for coffee and he's in a rush to get back for a meeting. The employee holds the door open, lets the person in and the unknown person interrupts his phone conversation to smile politely and say "Thank you."
>
> **Explanation:** The SE knows that most people are programmed to be helpful. The employee sees the man approach and realizes he can't reach for his swipe card in his pocket (not that he has one anyway!). The employee also hears familiar jargon, which makes them believe that the SE works for his company. The employee also sees that the SE is on the phone and society has programmed the employee that interrupting him to ask who he is or to show his pass would be rude and uncomfortable. The result is the SE walks into a secure building without being challenged and without having a swipe card. The polite "Thank you" from the SE to the victim provides the feedback/affirmation that the victim was looking for so they are left feeling as though they have carried out a good deed rather than just compromised their company's security.

The situation above is known as a **pretext**. A pretext is a scenario that is created by the SE to get a victim to do what they want, which in this case was to gain access to a building. A pretext can be a simple lie or story such as the SE has left their access pass at home or it can be as intricate as setting up a brand new identity or even impersonating someone such as a policeman or IT Help Desk engineer.

Exercise:

1. Create a list of three organizations that you would love to gain access to, stroll around, look at their internal network settings, and eat their donuts. The target organizations must be private, military, or "Mission Impossible" level, so choose well. Tell why you want to eat their donuts and which organizations you would pick. It's not like we are going to tell the police or anything, errr, maybe. Just kidding.
2. Describe several ways you might be able to gain access to each organization without going through the front door and not using any technology beyond a cell phone. Each organization requires at least one different approach to gain access. No repeating yourself. It's boring when you do.
3. If you must go through the building front door, you need to explain how you are going to get past the twenty-five burly security guards, their hungry attack dogs, and the eyes that never blink (security cameras).
   Be realistic. You are not a magician and the laws of physics apply. Your budget for each breach is $1,575 US. No, you do not own a helicopter or inviso-spray.

Who Uses Social Engineering and Why?

Social engineering is used every day by millions of people. Salespeople use SE to steer people into buying their products. Some of the best SEs are car dealers. Believe it or not, young kids are great at using SE to get what they want from their parents. "Mommy, I want this, I really, really need to have this, if I don't get this I'll cry." This scheme plays on our desire to please our kids and not have them scream in a store in front of everyone. Some people use SE to circumvent security and for malicious reasons but then others can put their skills to a more positive use. Which folks are "bad" and which ones are "good" in the list below? Does your answer depend on their goals?

Hackers	SE is usually used by hackers to circumvent security controls by manipulating the human, which is an easier target than secure IT systems.
Con Men/Identity Thieves	The term **con man** is actually short for "confidence man." A skilled con man, like any other social engineer, needs to gain the victims' confidence to deliver a successful pretext. Their aim is usually to exploit a victim's greed in order to profit themselves.
Sales People and Recruiters	Sales people and personnel recruiters or **headhunters** are experts at social engineering. Sales people use SE skills to extract information from you, and then sell you something based on this information. A headhunter might attempt to get a company's receptionist to provide them with a copy of the internal phone directory. Then they use that directory to target people with sought-after skills and lure them to another company – for a fat commission.
Other Groups and Organizations	Governments, criminal and terrorists organizations, cults, sexual predators; all of these groups use tools similar to the social engineers' to convince their targets to do what they want.

Other Professionals	Doctors, psychologists, lawyers, police investigators and interrogators all use a variety of social engineering techniques in order to extract information, manipulate their chosen target and achieve their desired outcome. Psychologists can use these skills to overcome people's fears, make them more confident or treat addiction.
Spies and Intelligence Services	Social engineering is a survival skill for spies and other intelligence operatives. Quite often their life depends on their ability to assume another identity, extract information or infiltrate a system or building. They use physical and psychological social engineering skills to stay alive and complete the mission that they have been assigned.

Social Engineering Method

OK, so now we know what SE is and why some folks prefer it over other methods to circumvent security. We also know the types of people that have these skills. But how do you carry out a social engineering attack?

Here's an overview of the approach often used by Social Engineers when engaging in an attack.

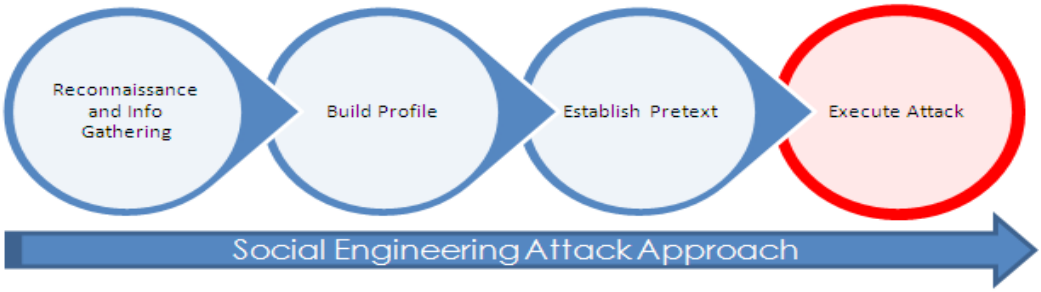


Figure 3: Social Engineering Attack Approach

Let's break the process down and take a look at each step:

Phase 1 - Reconnaissance and Information Gathering

Knowledge is power. Using a mixture of intelligence sources, a good SE builds a detailed profile of his target whether this is a company or a specific person. This profile allows him to get into the mind of the target. The results makes his pretext more convincing as he will be aware of details that give validity to his story; he's less likely to arouse suspicion and more likely to gain the trust and confidence of his target.

Open Source Intelligence (or **OSINT** as it's known in the intelligence world) is the phrase used to describe the collection and use of publicly available information. This type of info gathering is classed as **passive** because it doesn't involve directly interacting with the target. This is opposed to **active** gathering methods such as calling the target to try to extract information.

Online Information Sources

A whole book could be written on online sources of information. Below is a list of some of the more common examples that can be used for the information gathering phase.

Type of Site	Examples	Info to look for
Social Networking	www.facebook.com www.myspace.com www.twitter.com www.linkedin.com www.bebo.com www.friendsreunited.com www.blippy.com	Names, ages, date of birth, relatives, purchases, hobbies, favorite bands or other interests, GPS locations from check-ins and photo tags. LinkedIn can show systems in use, previous employment, colleagues, groups and associations…
Corporate and Employee Sites	www.victimcompany.com www.wordpress.com www.joe-employee.com	Share prices, organization charts, internal phone number ranges, email addresses, info on systems in use, company lingo…
Collaboration Web Sites	www.youtube.com www.pearltrees.com www.justgiving.com www.ebay.co.uk www.amazon.co.uk	Locations, hobbies, interests, purchases, charities victim is affiliated with, gift lists, book lists…
Network and System Sites	www.iana.com http://www.icann.org/ http://www.apnic.net/apnic-bin/whois.pl/ http://ws.arin.net/whois http://www.lacnic.net/ http://www.ripe.net/ http://centralops.net/co/ http://www.dnsstuff.com/ http://www.netcraft.com http://www.robtex.com/ http://www.archive.org/index.php	Company web sites, IP addresses, DNS servers, mail servers, ftp servers, software versions, security protection (such as anti-spam systems, anti-virus etc), databases in use, company location, data center location…
People and Company Directories	http://www.123people.com/ http://www.192.com/search/ http://www.411.com/ http://pipl.com/ http://www.spokeo.com/ http://www.zabasearch.com/%20 www.yell.com http://www.whitepages.com/	Company information, financial figures, organization charts, addresses, telephone numbers, email addresses...
Job Sites	www.monster.com www.jobserve.com www.indeed.com	Organization structure, financial information, systems in use, company policy, company terminology, salaries, email addresses...

Exercises:

1. Online Researching:
   A) Can you find any information that you think may be valuable to a SE?
   B) B) What could you do to stop a SE getting hold of this information?
   C) C) With a friend's permission test your skills on their trash and see if you can create a pretext from your findings that could be used to track them.How much information can you find out about yourself online?

Physical Reconnaissance

As well as gathering information online a lot of useful information can be gathered in the real world

1. **Surveillance**

Many social engineers will follow their target to learn how they operate, which locations they visit, do they smoke and so on. This information could be used to approach the target in a social manner to strike up a conversation. Do they carry keys, RFID cards or swipe cards? Do they drink and so may be vulnerable to giving away information while intoxicated?

2. **Dumpster Diving**

This is the fancy term given to rooting through the victim's trash. It is amazing what people throw away: bank statements, medical letters, bank cards, CD's, invoices and purchase records, diaries and contact lists; even computers.

Exercises:

D) Dumpster Dive
A) Explore your own trash. Can you find any information that you think may be valuable to a SE?
B) What could you do to stop a SE getting hold of this information?
C) With a friend's permission test your skills on their trash and see if you can create a pretext from your findings that could be used to track them.

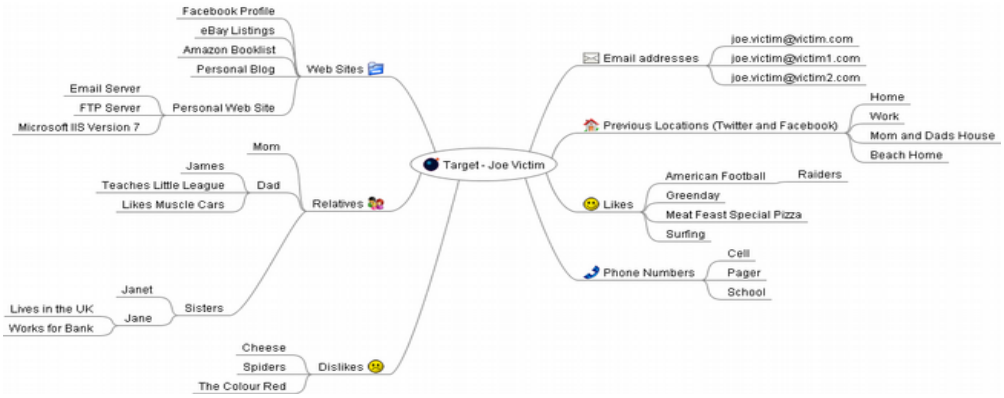
Phase 2 – Build a Profile

Phase 1 will generate a lot of information for the SE; being able to order it, record it and manipulate it is essential to utilize it effectively.

Building a mind map is a useful way to help present the information that you find in an orderly way. You can group information by source such as those presented in the table in 20.4.2; you could break it down into information types such as telephone numbers, email addresses, locations, likes, dislikes; the choice is yours.

Below is an example of one way you could build your target profile.

Figure 4: Target profiling using Freemind



Using the techniques detailed above, the SE is able to build a comprehensive picture of his victim. Who are they, what do they like, where do they hang out, who do they report to, what skills do they have, what frustrates them, what they want (wish lists and gift lists), what their ambitions are, when they are on holiday and where, where they live, what they buy and when. The list is endless and all this information makes it easy for a SE to create a convincing pretext in order to engage the victim and achieve his goal.

In previous lessons, you downloaded the BackTrack live CD. It contains the Social Engineer's Toolkit (SET). See if you can locate that application. Explore its capabilities. There are other information capture and organization tools for SEs. Search online for them and see what you find. You may wish to use one of those applications in the next exercise.

Exercises: Information Profiles at Work

1. Your first job out of high school is working for a tabloid and write exciting, mainly untrue stories about Hollywood people. Your task is to research someone who is popular now and write an outrageous story that can be backed up with 60% facts. Perhaps Michael Jackson has come back from the dead and fathered a child with an alien. Please use someone who is alive though.

2. Use the information that you have collected on your target to build a bold-faced lie story that could possibly happen. Ensure you have enough accurate details about your target to sound almost believable. Spin the details however you would like. The idea is to manipulate true information into a false story.

3. Photoshop a picture of the target that proves the story is accurate. Add a mustache to the picture, and a pirate patch over one eye.

Social Engineering: Real World Examples

To become a SE, you will need to change your whole personality or have the ability to change your personality when needed. Actors do this every day; they play a part and play it as convincingly as possible. An example for you to learn from is watching salespeople, preachers, marketers, ministers, public speakers, professional speakers, and politicians. They don't use technical jargon or talk down to the audience. No matter how big the crowd is, they are excellent at making each person feel as though they are talking just to them. The presenters make and keep eye contact; they do not refer to charts or pictures behind them.

Whether you are watching a salesperson trying to convince a couple to purchase a car or a televangelist, they are all trying to sell one main thing: themselves. Social engineers need to learn to sell themselves as well. You must be able to become a trustworthy and honest person with good intentions, just as a camouflage. Use visualization to place

yourself in the other person's mind. How would you react if some person asked for this or that? Look at your culture and your community for clues of what is acceptable behavior and what isn't.

Start by reading Dale Carnegie's *How to Win Friends and Influence People*. It is an old book but every word in it still applies today. If you go into a store wearing a tank top and worn out shoes, asking for a job, don't expect to be hired. Go into that same store with a fresh haircut (part on the left), a button down collar long sleeve shirt, nice pants with a matching belt, and some appropriate shoes and watch how you are treated so much nicer. "Perception is reality".

Learn to read body language and how to keep your body language from giving your scheme away. Whoever you are speaking to, look directly into their eyes. If you are trying to hide something, you will look up and to the left when asked a question. Focus on eye contact. Smell is another indicator that can help you. If you smell nice with fresh breath, you will gain attention and hold their attention for much longer than bad breath with smelly shoes. Search online for resources about body language. One author of note is Desmond Morris.

Take acting and speech class. Learn to act, though we don't expect you to perform in plays in the park on Saturday night. Actors are taught how to *project*; a speaking class will show you how to use inflection in your voice. You will want to practice in front of real people, not in a chat room.

Do not expect the phone to get you inside any organization. To the person on the other end of the phone, you are just another voice. Unless you have incredible speaking skills, leave the phone alone since calls can be traced and all calls to major organizations are recorded for "quality assurance". Yeah right. Calls are monitored and recoded for evidence as well as e-discovery. Person to person contacts are worth more to a SE for information, unless you are trying phishing with email. Those emails too are monitored and scanned by tiny ninjas who will come to your house and deflate your tires, eat all your favorite cereal, leave the freezer door open all day, and put bird droppings on your head as you walk (because of the deflated tires).

Exercises: Create a New You

Slowly change your appearance by parting your hair on the left, wearing cologne or perfume, put on a new shirt every day instead of once a week, and learn proper <insert your language here>. Good hygiene and manners will go a long way towards establishing yourself as a respectable person in public.
Now we need to change your mindset.

A. Everyone likes a good game of chance. Playing certain games such as poker (five card stud, Texas hold'em, Mexicali with dice) requires a bit more than just a good hand. In many betting games, you can bluff your way to win. Get a few friends who play nickel poker or some other game that you can try new personas on.
B. Every third or fourth hand, bluff. Take your bluff as far as you can without losing your shirt or lunch money. Don't make calculated bluffs, just use your instinct, use your gut or listen to that inner voice some of us hear. Ok, don't listen to all the voices, just the one that you trust. Build confidence, puff out your chest and look dazzling.
C. Try not to set a pattern for your bluffs, just try and use your worst cards to see how far you can last using your confidence, your body language, your voice tone and that ace you hid in your sock. Make everyone think that you know something or have something that they do not. Be devilish about it. Smirk, even if you lose, act like you meant to lose to set everyone else up on the next round. Confidence in the face of defeat is a great place to learn a "new you."

Further Reading

For an extensive glossary of terms visit the following URLs:

Maltego	http://www.paterva.com/web5/
Film – Catch me if you can	http://en.wikipedia.org/wiki/Catch_Me_If_You_Can
Social Engineering Blog – Security Through Education	http://www.social-engineer.org/blog/social-engineering/stealing-credentials-via-social-engineering/

Appendix 1: Internet Profile Form

Use the following form to record what information can be found on the Internet that relates to your target. Use the last column to list the things you could do to make the target safer. An example has been provided to get you started:

Site	Information Found	How can you protect against this?
www.facebook.com/johndoe999	Full name, maiden name, email address, telephone number, favorite band, 3 children jon, jane and bob	Ensure Facebook profile is set to friends only. Remove sensitive information such as bands and childrens names could be passwords.

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM