As already discussed social engineering can be used in many areas of life, but not all of these uses are malicious or bad. Many times social engineering can be used to motivate a person to take an action that is good for them. How? Th ink about this: John needs to lose weight. He knows he is unhealthy and needs to do something about it. All of John’s friends are overweight, too. They even make jokes about the joys of being overweight and say things like, “I love not worrying about my fi gure.” On one hand, this is an aspect of social engineering. It is social proof or consensus, where what you find or deem acceptable is determined by those around you. Because John’s close associations view being overweight as acceptable, it is easier for John to accept it. However, if one of those friends lost weight and did not become judgmental but was motivated to help, the possibility exists that John’s mental frame about his weight might change and he might start to feel that losing weight is possible and good. This is, in essence, social engineering. So you can clearly see how social engineering fi ts into society and everyday life, the following sections present a few examples of social engineering, scams, and manipulation and a review of how they worked.

**The 419 Scam** The 419 scam, better known as the Nigerian Scam, has grown into an epidemic. You can find an archived story and article about this scam at www.social-engineer.org/wiki/archives/ConMen/ConMen-Scam-NigerianFee.html. Basically an email (or as of late, a letter) comes to the target telling him he has been singled out for a very lucrative deal and all he needs to do is off er a little bit of help. If the victim will help the letter sender extract a large sum of money from foreign banks he can have a percentage. After the target is confident and “signs on,” a problem arises that causes the target to pay a fee. After the fee is paid another problem comes up, along with another fee. Each problem is “the last” with “one final fee” and this can be stretched out over many months. Th e victim never sees any money and loses from $10,000–$50,000 USD in the process. What makes this scam so amazing is that in the past, offi cial documents, papers, letterhead, and even face-to-face meetings have been reported. Recently a variation of this scam has popped up where victims are literally sent a real check. The scammers promise a huge sum of money and want in return only a small portion for their eff orts. If the target will wire transfer a small sum (in comparison) of $10,000, when they receive the promised check they can deposit the check and keep the difference. Th e problem is that the check that comes is a fraud and when the victim goes to cash it she is slapped with check fraud charges and fi nes, in some cases after the victim has already wired money to the scammer. Th is scam is successful because it plays on the victim’s greed. Who wouldn’t give $10,000 to make $1,000,000 or even $100,000? Most smart people would. When these people are presented with official documents, passports, receipts, and even official offi ces with “government personnel” then their belief is set and they will go to great lengths to complete the deal. Commitment and consistency play a part in this scam as well as obligation. I discuss these attributes in greater detail in later chapters, and when I do, you will see why this scam is so powerful. The Power of Scarcity The article archived at www.social-engineer.org/wiki/archives/Governments/ Governments-FoodElectionWeapon.html talks about a principle called scarcity. Scarcity is when people are told something they need or want has limited availability and to get it they must comply with a certain attitude or action. Many times the desired behavior is not even spoken, but the way it is conveyed is by showing people who are acting “properly” getting rewards. Th e article talks about the use of food to win elections in South Africa. When a group or person does not support the “right” leader, foodstuff s become scarce and jobs people once had are given to others who are more supportive. When people see this in action, it doesn’t take long to get them in line. Th is is a very malicious and hurtful form of social engineering, but nonetheless, one to learn from. It is often the case that people want what is scarce and they will do anything if they are lead to believe that certain actions will cause them to lose out on those items. What makes certain cases even worse, as in the earlier example, is that a government took something necessary to life and made it “scarce” and available only to supporters—a malicious, but very eff ective, manipulation tactic. The Dalai Lama and Social Engineering Th e interesting article archived at www.social-engineer.org/wiki/archives/ Spies/Spies-DalaiLama.html details an attack made on the Dalai Lama in 2009. A Chinese hacker group wanted to access the servers and fi les on the network owned by the Dalai Lama. What methods were used in this successful attack? Th e attackers convinced the offi ce staff at the Dalai Lama’s offi ce to download and open malicious software on their servers. Th is attack is interesting because it blends both technology hacking and social engineering. The article states, “The software was attached to e-mails that purported to come from colleagues or contacts in the Tibetan movement, according to researcher Ross Anderson, professor of security engineering at the University of Cambridge Computer Laboratory, cited by the Washington Times Monday. Th e software stole passwords and other information, which in turn gave the hackers access to the offi ce’s e-mail system and documents stored on computers there.” Manipulation was used as well as common attack vectors such as phishing (the practice of sending out emails with enticing messages and links or fi les that must be opened to receive more information; often those links or fi les lead to malicious payloads) and exploitation. Th is attack can work and has worked against major corporations as well as governments. Th is example is just one in a large pool of examples where these vectors cause massive damage. Employee Theft Th e topic of employee theft could fi ll volumes, especially in light of the staggering statistic found at www.social-engineer.org/wiki/archives/DisgruntledEmployees/ DisgruntledEmployees-EmployeeTheft.html that more than 60 percent of employees interviewed admitted to taking data of one sort or another from their employers. Many times this data is sold to competitors (as happened in this story from a Morgan Stanley employee: www.social-engineer.org/wiki/archives/ DisgruntledEmployees/DisgruntledEmployees-MorganStanley.html). Other times employee theft is in time or other resources; in some cases a disgruntled employee can cause major damage. I once talked to a client about employee discharge policies, things like disabling key cards, disconnecting network accounts, and escorting discharged employees out of the building. Th e company felt that everyone was part of the “family” and that those policies wouldn’t apply. Unfortunately, the time came to let go of “Jim,” one of the higher-ranking people in the company. Th e “fi ring” went well; it was amicable and Jim said he understood. Th e one thing the company did right was to handle the fi ring around closing time to avoid embarrassment and distraction. Hands were shook and then Jim asked the fateful question, “Can I take an hour to clean out my desk and take some personal pictures off my computer? I will turn my key card into the security guard before I leave.” Feeling good about the meeting, they all quickly agreed and left with smiles and a few laughs. Th en Jim went to his office, packed a box of all his personal items, took the pictures and other data off his computer, connected to the network, and wiped clean 11 servers’ worth of data—accounting records, payroll, invoices, orders, history, graphics, and much more just deleted in a matter of minutes. Jim turned in his key card as he promised and calmly left the building with no proof that he was the one to initiate these attacks. Th e next morning a call came in to me from the owner describing the carnage in the ex-employee’s wake. Hoping for a silver bullet, the client had no choice but try to recover what could be recovered forensically and start over from the backups, which were more than two months old. A disgruntled employee who is left unchecked can be more devastating than a team of determined and skilled hackers. To the tune of $15 billion USD, that is what the loss is estimated at being to businesses in the U.S. alone due to employee theft. Th ese stories may leave a question about what diff erent categories of social engineers are out there and whether they can be classifi ed. DarkMarket and Master Splynter In 2009 a story broke about an underground group called DarkMarket—the socalled eBay for criminals, a very tight group that traded stolen credit card numbers and identity theft tools, as well as the items needed to make fake credentials and more. An FBI agent by the name of J. Keith Mularski went under deep cover and infi ltrated the DarkMarket site. After a while, Agent Mularski was made an administrator of the site. Despite many trying to discredit him he hung in for more than three years as the admin of the site. During this time, Mularski had to live as a malicious hacker, speak and act as one, and think as one. His pretext was one of a malicious spammer and he was knowledgeable enough to pull it off . His pretext and his social engineering skills paid off because Agent Mularski infi ltrated DarkMarket as the infamous Master Splynter, and after three years was essential in shutting down a massive identity theft ring. Th e three-year social engineering sting operation netted 59 arrests and prevented over $70 million in bank fraud. Th is is just one example of how social engineering skills can be used for good. The Different Types of Social Engineers As previously discussed, social engineering can take on many forms. It can be malicious and it can be friendly, it can build up and it can tear down. Before moving on to the core of this book, take a brief look at the diff erent forms of social engineers and a very short description of each: » Hackers: Software vendors are becoming more skilled at creating software that is hardened, or more diffi cult to break into. As hackers are hitting more hardened software and as software and network attack vectors, such as remote hacking, are becoming more diffi cult, hackers are turning to social engineering skills. Often using a blend of hardware and personal skills, hackers are using social engineering in major attacks as well as in minor breaches throughout the world. » Penetration testers: Since a real-world penetration tester (also known as a pentester) is very off ensive in nature, this category must follow after hackers. True penetration testers learn and use the skills that the malicious hackers use to truly help ensure a client’s security. Penetration testers are people who might have the skills of a malicious black hat but who never use the information for personal gain or harm to the target. » Spies: Spies use social engineering as a way of life. Often employing every aspect of the social engineering framework (discussed later in this chapter), spies are experts in this science. Spies from all around the world are taught diff erent methods of “fooling” victims into believing they are someone or something they are not. In addition to being taught the art of social engineering, many times spies also build on credibility by knowing a little or even a lot about the business or government they are trying to social engineer. » Identity thieves: Identity theft is the use of information such as a person’s name, bank account numbers, address, birth date, and social security number without the owner’s knowledge. Th is crime can range from putting on a uniform to impersonating someone to much more elaborate scams. Identity thieves employ many aspects of social engineering and as time passes they seem more emboldened and indiff erent to the suff ering they cause. » Disgruntled employees: After an employee has become disgruntled, they often enter into an adversarial relationship with their employer. Th is can often be a one-sided situation, because the employee will typically try to hide their level of displeasure to not put their employment at risk. Yet the more disgruntled they become, the easier it becomes to justify acts of theft, vandalism, or other crimes. » Scam artist: Scams or cons appeal to greed or other principles that attract people’s beliefs and desires to “make a buck.” Scam artists or con men master the ability to read people and pick out little cues that make a person a good “mark.” Th ey also are skillful at creating situations that present as unbeatable opportunities to a mark. » Executive recruiters: Recruiters also must master many aspects of social engineering. Having to master elicitation as well as many of the psychological principles of social engineering, they become very adept at not only reading people but also understanding what motivates people. Many times a recruiter must take into consideration and please not only the job seeker but also the job poster. » Salespeople: Similar to recruiters, salespeople must master many people skills. Many sales gurus say that a good salesperson does not manipulate people but uses their skills to fi nd out what people’s needs are and then sees whether they can fi ll it. Th e art of sales takes many skills such as information gathering, elicitation, infl uence, psychological principles, as well as many other people skills. » Governments: Not often looked at as social engineers, governments utilize social engineering to control the messages they release as well as the people they govern. Many governments utilize social proof, authority, and scarcity to make sure their subjects are in control. Th is type of social engineering is not always negative, because some of the messages governments relay are for the good of the people and using certain elements of social engineering can make the message more appealing and more widely accepted. » Doctors, psychologists, and lawyers: Although the people in these careers might not seem like they fi t into the same category as many of these other social engineers, this group employs the same methods used by the other groups in this list. Th ey must use elicitation and proper interview and interrogation tactics as well as many if not all of the psychological principles of social engineering to manipulate their “targets” (clients) into the direction they want them to take. Regardless of the fi eld, it seems that you can fi nd social engineering or an aspect of it. Th is is why I hold fi rmly to the belief that social engineering is a science. Set equations exist that enable a person to “add up” elements of social engineering to lead to the goal. In the example of a con man, think of the equation like this: pretext + manipulation + attachment to greed = target being social engineered. In every situation, knowing what elements will work is the hard part, but then learning how to utilize those elements is where the skill comes in. Th is was the basis for thought behind developing the social engineering framework. Th is framework has revolutionized the way social engineering is dissected, as discussed in the next section. The Social Engineering Framework and How to Use It Th rough experience and research I have tried to outline the elements that make up a social engineer. Each of these elements defi nes a part of the equation that equals a whole social engineer. Th ese aspects are not set in stone; as a matter of fact, from its original state until now the framework has grown. Th e purpose of the framework is to give enough information for anyone to build on these skills. Th e framework is not designed to be an all-inclusive resource for all information in each chapter. For example, the portion of Chapter 5 that covers microexpressions is based on the research of some of the greatest minds in this fi eld and my experience in using that information. By no means is it meant to replace the 50 years of research by such great minds as Dr. Paul Ekman. As you read through the framework you will see that by utilizing the many skills within it, you can not only enhance your security practice, but also your mindset about how to remain secure, how to communicate more fully, and how to understand how people think. Refer to the table of contents for a clear picture of the framework or view it online at www.social-engineer.org/framework. At fi rst glance the framework may appear daunting, but inside this book you will fi nd an analysis of each topic that will enable you to apply, enhance, and build these skills. Knowledge is power—it is true. In this sense, education is the best defense against most social engineering attacks. Even the ones that knowledge can’t protect 100 percent against, having details of these attacks keeps you alert. Education can help you enhance your own skills, as well as be alert. Along with education, though, you need practice. Th is book was not designed to be a once-read manual; instead it was designed to be a study guide. You can practice and customize each section for your needs. Th e framework is progressive in the sense that it is the way a social engineering attack is laid out. Each section of the framework discusses the next topic in the order that a social engineer might utilize that skill in their engagement or planning phases. The framework shows how an attack might be outlined. After the attack is planned out, the skills that are needed can be studied, enhanced, and practiced before delivery. Suppose, for example, that you are planning a social engineering audit against a company that wanted to see whether you could gain access to its server room and steal data. Maybe your plan of attack would be to pretend to be a tech support person who needs access to the server room. You would want to gather information, maybe even perform a dumpster dive. Th en under the pretext of being the tech guy, you could utilize some covert camera tools as well as practice the proper language and facial/vocal cues for how to act, sound, and look like a tech guy. If you locate what company your client uses for tech support you may need to do info gathering on it. Who does your client normally get to service them? What are the names of the employees with whom they interact? Th e attack needs to be planned out properly. Th is book is not just for those who perform audits, though. Many readers are curious about what the attacks are, not because they are protecting a company, but because they need to protect themselves. Not being aware of the way a malicious social engineer thinks can lead someone down the path toward being hacked. College students in the fi eld of security have also used the framework. Th e information in the framework outlines a realistic path for these vectors, or methods of attack, and enables the reader to study them in depth. Generally, this information can also help enhance your ability to communicate in everyday life. Knowing how to read facial expressions or how to use questions to put people at ease and elicit positive responses can enhance your ability to communicate with your family and friends. It can assist you in becoming a good listener and more aware of people’s feelings. Being able to read people’s body language, facial expressions, and vocal tones can also enhance your ability to be an eff ective communicator. Understanding how to protect yourself and your loved ones will only make you more valuable and more aware of the world around you.

**Gathering Information**

Gathering information is like building a house. If you try to start with the roof your house will surely be a failure. A good house will be built using a solid foundation and from there it will be built literally from the ground up. As you gather information you may be overwhelmed with how to organize and then use this data, so starting a fi le or an information gathering service to gather this data in is a good idea. Many tools exist to assist in collecting and then using this data. For penetration tests and social engineering audits I use a Linux distribution called BackTrack that is specifi cally designed for this purpose. BackTrack is like most Linux distributions in that it is free and open source. Perhaps its greatest asset is that it contains more than 300 tools designed to assist in security auditing. All of the tools within BackTrack are also open source and free. Especially attractive is the high quality of BackTrack’s tools, many of which rival and even surpass tools you would pay an arm and a leg for. Two BackTrack tools that are particularly useful for information gathering and storing are called Dradis and BasKet. Th e following sections take a quick look at each.

Using BasKet BasKet is similar in functionality to Notepad, but more like Notepad on steroids. It is presently maintained by Kelvie Wong and can be found for free either in BackTrack or at http://basket.kde.org/. Th e website has full instructions for how to install BasKet. Once installed BasKet is easy to use and the interface is not diffi cult to understand. As seen in Figure 2-1, the interface is easy to fi gure out. Adding a new “Basket” to hold data is as simple as right clicking on the left side of the screen and selecting New Basket. Once new Baskets are added the sky is the limit. You can copy and paste data, place screen shots in the Basket, or even tie in OpenOffi ce or other types of charts, graphs, and other utilities. Th e easiest is to copy the image then right mouse click on the new Basket and click Paste. As shown in Figure 2-1, adding images is simple but also shows the image right away. Notes can be typed or pasted around the images by simply clicking in the Basket and starting to type. In a normal security audit, what makes BasKet attractive is the way it catalogs data and shows it on the screen. I usually add a diff erent Basket for each type of data such as Whois, social media, and so on. After that, I will do some recon using Google Maps or Google Earth to capture some images of the client’s building or facility, which I can store in BasKet as well. When the audit is complete, being able to pull up and utilize this information quickly is very easy. Figure 2-2 illustrates a nearly complete BasKet that contains a lot of useful information and tabs. As shown in Figure 2-2, BasKet is easy to store the information in an easy-to-read format. I try to include as much information as possible because no information is too small to store. Th e information I include is items from the client’s website, WhoIs information, social media sites, images, employee contact info, resumes found, forums, hobbies, and anything else I fi nd linked to the company. When I am done, I simply click on the menu called Basket then Export and export the whole BasKet as an HTML page. Th is is great for reporting or sharing this data. For a social engineer, collecting data, as will be discussed in detail later, is the crux of every gig, but if you cannot recall and utilize the data quickly, it becomes useless. A tool like BasKet makes retaining and utilizing data easy. If you give BasKet a try and use it once, you will be hooked.

Using Dradis Although BasKet is a great tool, if you do a lot of information gathering, or if you work on team that needs to collect, store, and utilize data, then a tool that allows for multi-user sharing of this data is important. Enter Dradis. According to the creators of the open-source Dradis, the program is a “self-contained web application that provides a centralized repository of information” you have gathered, and a means by which to plan for what’s to come. Like BasKet, Dradis is a free, open-source tool that can be found at http:// dradisframework.org/. Whether you are using Linux, Windows, or a Mac, Dradis has easy-to-use set up and installation instructions found at http://dradisframework .org/install.html. Once Dradis is installed and set up, you simply browse to the localhost and port you assigned, or use the standard 3004. You can do this by opening a browser and typing https://localhost:3004/. Once logged in, you’re greeted with the screen shown in Figure 2-3. Notice the Add Branch button at the top left. Adding a branch allows you to add similar details as you can in BasKet: notes, images, and more, and you can even import notes. Dradis and BasKet are just two tools that I have used to collect and store data. Th e websites for both Dradis and BasKet have very nice tutorials on setting up and using these powerful tools. Whatever operating system you use—Mac, Windows, or Linux—there are choices out there for you. What is important is to use a tool that you are comfortable with and that can handle large amounts of data. For that reason I suggest staying away from things like Notepad in Windows or Smultron or TextEdit in Mac. You want to be able to format and highlight certain areas to make them stand out. In my Dradis server, pictured in Figure 2-3, I have a section for phone scripts. Th is functionality is handy for transcribing ideas that might work based on the information I gathered. Th ese tools suggest how a social engineer begins to utilize the information he collects. Th e fi rst stage in utilizing the information you gather is thinking like a social engineer.

**Thinking Like a Social Engineer** Having a few hundred megabytes of data and pictures is great, but when you start reviewing it, how do you train yourself to review and then think of the data in a way that has maximum impact? Of course you could just open a browser and type in long-winded random searches that may lead to some form of information, some of which may even be useful. If you are hungry you probably don’t just run to the kitchen and start to throw whatever ingredients you see into a bowl and start digging in. Planning, preparation, and thought all cause the meal to be good. Similar to a real meal, a social engineer needs to plan, prepare, and think about what information he will try to obtain and how he will obtain it. When it comes to this vital step of information gathering many people will have to change the way they think. You have to approach the world of information in front of you with a diff erent opinion and mindset than what you normally may have. You have to learn to question everything, and, when you see a piece of information, learn to think of it as a social engineer would. Th e way you ask questions of the web or other sources must change. Th e way you view the answers that come back must also change. Overhearing a conversation, reading what seems like a meaningless forum post, seeing a bag of trash—you should assimilate this information in a diff erent way than you did before. My mentor Mati gets excited when he sees a program crash. Why? Because he is a penetration tester and exploit writer. A crash is the fi rst step to fi nding a vulnerability in software, so instead of being irritated at losing data he gets excited at the crash. A social engineer must approach information in much the same way. When fi nding a target that utilizes many diff erent social media sites, look for the links between them and the information that can create a whole profi le. As an example, one time I rented a car to drive a few states away for business. My companion and I loaded all of our luggage in the trunk; as we were entering the car we noticed a small bag of trash in the back seat. Th e other person said something like, “Service today just stinks. You fi gure for what you pay they would at least clean out the car.” True, you would expect that, but I stopped that bag from just being chucked into the nearest can, and I said, “Let me just look at that really quick.” As I opened the bag and pushed aside the Taco Bell wrappers, what was lying in plain sight was a shock to me—half of a ripped-up check. I quickly dumped out the bag and found a bank receipt and the other half of the check. Th e check was written out for a couple thousand dollars, then just ripped up—not into tiny little pieces, but just into four large chunks, then thrown into a small bag with a Taco Bell wrapper. Taping it back together revealed this person’s name, company name, address, phone number, bank account number, and bank routing number. Together with the bank receipt I now had the balance of his account. Th ankfully for him I am not a malicious person because only a couple more steps are needed to commit identity theft. Th is story personifi es how people view their valuable information. Th is guy rented the car before me and then because he threw the check away he felt it was gone, disposed of safely. Or so he thought; but this is not an isolated case. At this URL you can fi nd a recent story about very valuable things people just threw away or sold for next to nothing at a garage sale: www.social-engineer.org/wiki/ archives/BlogPosts/LookWhatIFound.html. If people throw away a painting with a hidden copy of the Declaration of Independence in it, then throwing away bills, medical records, old invoices, or credit card statements probably isn’t such a huge deal. How you interact with people in public can have devastating eff ects. In the following scenario I was asked to audit a company and before I could proceed I needed to gather some data. Take a look at how simple, seemingly meaningless information can lead to a breach. Simply following one of the higher ups of the target company for a day or two showed me that he stopped for coff ee every morning at the same time. Since I was aware of his 7:30 a.m. coff ee stop at the local coff ee shop I could plan a “meeting.” He would sit for 30–35 minutes, read the paper, and drink a medium cafe latte. I enter the shop about 3–5 minutes after he sits down. I order the same drink as him and sit down next to him in the shop. I look over as he places one section of the paper down and ask whether I can read the paper he is done with. Having already picked up a paper on the way I knew that page three contained an article about a recent murder in the area. After acting as if I just read it, I say out loud, “Even in these small towns things are scary nowadays. You live around here?” Now at this point the target can blow me off , or if I played my cards right, my body language, vocal tone, and appearance will put him at ease. He says, “Yeah, I moved in a few years back for a job. I like small towns, but you hear this more and more.”

I continue, “I am just traveling through the area. I sell high-end business consulting services to large companies and always enjoy traveling through the smaller towns but I seem to hear more and more of these stories even in the rural areas.” Th en in a very joking tone I say, “You don’t happen to be a bigwig in a large company that needs some consulting do you?” He laughs it off and then as if I just challenged him to prove his worth says, “Well I am a VP of fi nance at XYZ Corp. here locally, but I don’t handle that department.” “Hey, look, I am not trying to sell you something, just enjoy coff ee, but if you think I can stop by and leave you some information tomorrow or Wednesday?” Th is is where the story gets interesting, as he says, “Well I would but I am heading out for a much-needed vacation on Wednesday. But why don’t you mail it to me and I will call you.” He then hands me a card. “Going somewhere warm and sunny, I hope?” I ask this knowing that I am probably getting close to my point where I need to cut it off . “Taking the wife on a cruise south.” I can tell he doesn’t want to tell me where, which is fi ne, so we shake hands and part ways. Now could he have been blowing me off ? Probably, but I have some valuable information: » His direct number » When he is leaving for vacation » What type of vacation » Th at he is local » Th e name of his company » His title in his company » Th at he recently relocated Of course, some of this information I already had from previous information gathering, but I was able to add a substantial amount to it after this meeting. Now to launch the next part of the attack, I call his direct line the day after he is supposed to be gone and ask for him, only to be told by his receptionist, “Sorry, Mr. Smith is on vacation—can I take a message?” Excellent. Th e information is verifi ed and now all I need to do is launch the fi nal phase, which means dressing up in a suit and taking my $9 business cards to his offi ce. I enter, sign in, and tell the receptionist I have an appointment with Mr. Smith at 10:00 a.m. To which she replies, “He is on vacation, are you sure it is today?

Using my practice sessions on microexpressions, a topic addressed in Chapter 5, I show true surprise: “Wait, his cruise was this week? I thought he left next week.” Now this statement is vital—why? I want the appointment to be believable and I want the receptionist to trust me by proxy. By stating I know about his cruise this must mean Mr. Smith and I have had intimate conversation—enough so that I know his itinerary. But my helplessness elicits pity and right away the secretary comes to my aid. “Oh, honey, I am sorry, do you want me to call his assistant?” “Ah, no.” I reply. “I really wanted to leave some information with him. How about this—I will just leave it with you and you can give it to him when he gets back? I am terribly embarrassed; maybe you can avoid even telling him I did this?” “My lips are sealed.” “Th ank you. Look I am going to crawl out of here, but before I do can I just use your bathroom?” I know that I normally would not be buzzed in, but I hope the combination of my rapport, my helplessness, and their pity will lead to success—and it does. While in the bathroom, I place an envelope in one stall. On the cover of the envelope I put a sticker that says PRIVATE. Inside the “private” envelope is a USB key with a malicious payload on it. I do this in one stall and also in the hallway by a break room to increase my chances and hope that the person that fi nds one of them is curious enough to insert it into their computer. Sure enough, this method seems to always work. Th e scary thing is that this attack probably wouldn’t work if it weren’t for a useless little conversation in a coffee shop. Th e point is not only about how small data can still lead to a breach, but also how you collect this data. Th e sources that you can use to collect data are important to understand and test until you are profi cient with each method and each source of collection. Th ere are many diff erent types of sources for collecting data. A good social engineer must be prepared to spend some time learning the strengths and weaknesses of each as well as the best way to utilize each source. Th us the topic of the next section.

**Whois Reconnaissance** Whois is a name for a service and a database. Whois databases contain a wealth of information that in some cases can even contain full contact information of the website administrators. Using a Linux command prompt or using a website like www.whois.net can lead you to surprisingly specifi c results like such as a person’s email address, telephone number, or even DNS server IP address. Whois information can be very helpful in profi ling a company and fi nding out details about their servers. All of this information can be used for further information gathering or to launch social engineering attacks.

Public Servers A company’s publicly reachable servers are also great sources for what its websites don’t say. Fingerprinting a server for its OS, installed applications, and IP information can say a great deal about a company’s infrastructure. After you determine the platform and applications in use, you could combine this data with a search on the corporate domain name to fi nd entries on public support forums. IP addresses may tell you whether the servers are hosted locally or with a provider; with DNS records you can determine server names and functions, as well as IPs. In one audit after searching the web using the tool called Maltego (discussed in Chapter 7), I was able to uncover a publicly facing server that housed literally hundreds of documents with key pieces of information about projects, clients, and the creators of those documents. Th is information was devastating to the company. An important note to keep in mind is that performing a port scan—using a tool like NMAP or another scanner to locate open ports, software, and operating systems used on a public server—can lead to problems with the law in some areas. For example, in June 2003, an Israeli, Avi Mizrahi, was accused by the Israeli police of the off ense of attempting the unauthorized access of computer material. He had port scanned the Mossad website. About eight months later, he was acquitted of all charges. Th e judge even ruled that these kinds of actions should not be discouraged when they are performed in a positive way (www.law.co.il/media/ computer-law/mizrachi\_en.pdf). In December 1999, Scott Moulton was arrested by the FBI and accused of attempted computer trespassing under Georgia’s Computer Systems Protection Act and Computer Fraud and Abuse Act of America. At the time, his IT service company had an ongoing contract with the Cherokee County of Georgia to maintain and upgrade the 911 center security (www.securityfocus.com/news/126). As part of his work, Moulton performed several port scans on Cherokee County servers to check their security and eventually port scanned a web server monitored by another IT company. Th is provoked a lawsuit, although he was acquitted in 2000. Th e judge ruled that no damage occurred that would impair the integrity and availability of the network. In 2007 and 2008, England, France, and Germany passed laws that make unlawful the creation, distribution, and possession of materials that allow someone to break any computer law. Port scanners fall under this description. Of course, if you are involved in a paid audit of a company most of this will be in the contract, but it is important to state that it is up to the social engineer auditor to be aware of the local laws and make sure you are not breaking them.

**Social Media** Many companies have recently embraced social media. It’s cheap marketing that touches a large number of potential customers. It’s also another stream of information from a company that can provide breadcrumbs of viable information. Companies publish news on events, new products, press releases, and stories that may relate them to current events. Lately, social networks have taken on a mind of their own. When one becomes successful it seems that a few more pop up that utilize similar technology. With sites like Twitter, Blippy, PleaseRobMe, ICanStalkU, Facebook, LinkedIn, MySpace, and others, you can fi nd information about people’s lives and whereabouts in the wide open. Later, this book will discuss this topic in much more depth and you will see that social networks are amazing sources of information.

**User Sites, Blogs, and So On** User sites such as blogs, wikis, and online videos may provide not only information about the target company, but also off er a more personal connection through the user(s) posting the content. A disgruntled employee who’s blogging about his company’s problems may be susceptible to a sympathetic ear from someone with similar opinions or problems. Either way, users are always posting amazing amounts of data on the web for anyone to see and read. Case in point: Take a look at a new site that has popped up—www.icanstalku .com (see Figure 2-4). Contrary to its name, it does not encourage people to actually stalk others. Th is site points to the complete thoughtlessness of many Twitter users. It scrapes the Twitter site and looks for users who are silly enough to post pictures using their smart phones. Many people do not realize that most smart phones embed GPS location data in their photos. When a user posts a picture to the web with this data embedded it can lead a person right to their location. Displaying location-based information is a scary aspect of social media websites. Not only do they allow you to post pictures of yourself, they also implicitly reveal your location—possibly without your knowledge. Sites like ICanStalkU underscore the danger of this information. Check out a story (one of many) that shows how this data is used for home break-ins, robberies, and sometimes more at www.social-engineer.org/wiki/archives/BlogPosts/ TwitterHomeRobbery.html. Th is type of information can give you a very detailed profi le of your target. People love to tweet about where they are, what they are doing, and who they are with. Blippy allows a person to connect their bank accounts and in essence it will “tweet” with each purchase, where it was from, and how much it costs. With pictures including embedded location data and then sites like Facebook, which many use to put personal pictures, stories, and other related info, it is a social engineer’s dream. In a short while a whole profi le can be developed with a person’s address, job, pictures, hobbies, and more. Another aspect of social media sites that makes them excellent sources of information gathering is the ability to be anonymous. If the target is a recently divorced middle-aged man who loves his Facebook page, you can be a young woman who is looking for a new friend. Many times, while fl irting, people divulge valuable pieces of information. Combine the ability to be anyone or anything you want on the web with the fact that most people believe everything they read as gospel fact and what you have is one of the greatest risks to security.

**Public Reports** Public data may be generated by entities inside and outside the target company. Th is data can consist of quarterly reports, government reports, analyst reports, earnings posted for publicly traded companies, and so on. An example of these are Dunn and Bradstreet reports or other sales reports that are sold for very little money and contain a lot of details on the target company. Another avenue discussed in more detail later is using background checkers such as those found at www.USSearch.com and www.intelius.com. Th ese sites, along with many others, can off er background check services for as little as $1 for one limited report to a $49 per month fee that lets you run as many checks as you want. You can get much of this information for free using search engines, but some of the detailed fi nancial data and personal information can only be obtained easily and legally through a paid-for service. Perhaps most shocking is that many of these companies may even provide data like a person’s Social Security Number to some customers**.**

**Using the Power of Observation** Though not used enough as a social engineering tool, simple observation can tell you much about your target. Does the target’s employees use keys, RFID cards, or other methods to enter the building? Is there a designated area for smoking? Are dumpsters locked, and does the building have external cameras? External devices such as power supplies or air conditioning units usually reveal who the service company is, and that can allow the social engineer another vector to gain access. Th ese are just a few of the questions that you can get answers for through observation. Taking some time to watch the target, fi lm using a covert camera, and then studying and analyzing the information later can teach you a lot and give your information fi le a major boost.

**Going through** the Garbage Yes, as hard as it is to imagine enjoying jumping through the trash, it can yield one of the most lucrative payoff s for information gathering. People often throw away invoices, notices, letters, CDs, computers, USB keys, and a plethora of other devices and reports that can truly give amazing amounts of information. As mentioned previously, if people are willing to throw away art that is worth millions, then things they view as trash will often go without a second thought, right into the garbage. Sometimes companies shred documents they deem as too important to just throw out, but they use an ineffi cient shredder that leaves paper too easy to put back together, as shown in Figure 2-5. This type of shredding can be thwarted with a little time and patience and some tape, as seen in Figure 2-6. Documents that can be even partially taped back together can reveal some very devastating information.

However, using a shredder that shreds both directions into a fi ne minced mess makes taping documents back together nearly impossible, as shown in Figure 2-7. Many companies use commercial services that take their shredded documents away for incineration. Some companies even leave the shredding to a third party, which, as you probably guessed, leaves them open to another attack vector. A social engineer who fi nds out the name of their vendor for this can easily mimic the pickup person and be handed all their documents. Nevertheless, dumpster diving can off er a quick way to fi nd all the information you want. Remember some key pointers when performing a dumpster dive: » Wear good shoes or boots: Nothing will ruin your day faster than jumping in a dumpster and having a nail go through your foot. Make sure your shoes tie on nice and tight as well as off er protection from sharp objects. » Wear dark clothing: Th is doesn’t need much explanation. You probably want to wear clothes you don’t mind having to get rid of, and dark clothes to avoid being detected. » Bring a fl ashlight » Grab and run: Unless you are in such a secluded area that you have no chance of being caught, grabbing some bags and going elsewhere to rummage through them might be best. Dumpster diving almost always leads to some very useful information. Sometimes a social engineer doesn’t even have to dive into a dumpster to fi nd the goods. Already mentioned in Chapter 1 is the article found at www.social-engineer .org/resources/book/TopSecretStolen.htm, but it solidifi es this thought. Th e Canadian CTU (Counter-Terrorism Unit) had plans for a new building that outlined its security cameras, fences, and other top-secret items. Th ese blueprints were just thrown away—yes, just tossed in the trash, not even shredded, and fortunately found by a friendly person. Th is story is just one of many that show “the height of stupidity,” as the article stated, but from a social engineer’s point of view, trash diving is one of the best information gathering tools out there.

**Using Profiling Software** Chapter 7 discusses the tools that make up some of the professional toolsets of social engineers, but this section off ers a quick overview. Password profi lers such as Common User Passwords Profi ler (CUPP) and Who’s Your Daddy (WYD) can help a social engineer profi le the potential passwords a company or person may use. How to use these tools is discussed in Chapter 7, but a tool like WYD will scrape a person or company’s website and create a password list from the words mentioned on that site. It is not uncommon for people to use words, names, or dates as passwords. Th ese types of software make it easy to create lists to try. Amazing tools such as Maltego (see Chapter 7 for more details), made by Paterva, are an information gatherer’s dream. Maltego allows a social engineer to perform many web-based and passive information gathering searches without having to use any utilities but Maltego itself. Th en it will store and graph this data on the screen to be used in reporting, exporting or other purposes. This can really help in developing a profile on a company. Remember, your goal as you collect data is to learn about the target company and the people within the company. Once a social engineer collects enough data, a clear picture will form in their minds as to the best way to manipulate the data from the targets. You want to profi le the company as a whole and fi nd out roughly how many employees are part of some club, a hobby, or group. Do they donate to a certain charity or do their kids go to the same school? All of this information is very helpful in developing a profi le. A clear profi le can help the social engineer not only in developing a good pretext, but can also outline what questions to use, what are good or bad days to call or come onsite as well as many other clues that can make the job so much easier. All of the methods discussed so far are mostly physical, very personal methods of information gathering. I didn’t touch on the very technical side of information gathering like services such as SMTP, DNS, Netbios, and the almighty SNMP. I do cover some of the more technical aspects that Maltego can help with in Chapter 7 in more detail. Th ese methods are worth looking into but are very much technical in nature as opposed to more “human” in nature. Whatever the method you utilize to gather information logically, the question that may come up is now that you know where to gather, how to gather, and even how to catalog, store, and display this info, what do you do with it? As a social engineer, after you have information you must start planning your attacks. To do that you need to start modeling an outline that will use this information. One of the best ways to start utilizing this data is to develop what is called a communication model.

**Communication Modeling** The more elaborate our means of communication, the less we communicate. —Joseph Priestley Communication is a process of transferring information from one entity to another. Communication entails interactions between at least two agents, and can be perceived as a two-way process in which there is an exchange of information and a progression of thoughts, feelings, or ideas toward a mutually accepted goal or direction. Th is concept is very similar to the defi nition of social engineering, except the assumption is that those involved in the communication already have a common goal, whereas the goal of the social engineer is to use communication to create a common goal. Communication is a process whereby information is enclosed in a package and is channeled and imparted by a sender to a receiver via some medium. Th e receiver then decodes the message and gives the sender feedback. All forms of communication require a sender, a message, and a receiver. Understanding how communication works is essential to developing a proper communication model as a social engineer. Modeling your communication as a social engineer will help us to decide the best method of delivery, the best method for feedback, and the best message to include. Communication can take many diff erent forms. Th ere are auditory means, such as speech, song, and tone of voice, and there are nonverbal means, such as body language, sign language, paralanguage, touch, and eye contact. Regardless of the type of communication used, the message and how it is delivered will have a defi nite eff ect on the receiver. Understanding the basic ground rules is essential to building a model for a target. Some rules cannot be broken, such as communication always has a sender and a receiver. Also everyone has diff erent personal realities that are built and aff ected by their past experiences and their perceptions. Everyone perceives, experiences, and interprets things diff erently based on these personal realities. Any given event will always be perceived diff erently by diff erent people because of this fact. If you have siblings, a neat exercise to prove this is to ask them their interpretation or memory of an event, especially if it is an emotional event. You will see that their interpretation of this event is very diff erent from what you remember. Each person has both a physical and a mental personal space. You allow or disallow people to enter that space or get close to you depending on many factors. When communicating with a person in any fashion, you are trying to enter their personal space. As a social engineer communicates they are trying to bring someone else into their space and share that personal reality. Eff ective communication attempts to bring all participants into each other’s mental location. Th is happens with all interactions, but because it is so common people do it without thinking about it. In interpersonal communications two layers of messages are being sent: verbal and nonverbal. Communication usually contains a verbal or language portion, whether it is in spoken, written, or expressed word. It also usually has a nonverbal portion—facial expressions, body language, or some non-language message like emoticons or fonts. Regardless of the amount of each type of cue (verbal or nonverbal), this communication packet is sent to the receiver and then fi ltered through her personal reality. She will form a concept based on her reality, then based on that will start to interpret this packet. As the receiver deciphers this message she begins to unscramble its meaning, even if that meaning is not what the sender intended. Th e sender will know whether his packet is received the way he intended if the receiver gives a communication packet in return to indicate her acceptance or denial of the original packet. Here the packet is the form of communication: the words or letters or emails sent. When the receiver gets the message she has to decipher it. Many factors depend on how it is interpreted. Is she in a good mood, bad mood, happy, sad, angry, compassionate—all of these things as well as the other cues that alter her perception will help her to decipher that message. Th e social engineer’s goal has to be to give both the verbal and nonverbal cues the advantage to alter the target’s perception so as to have the impact the social engineer desires. Some more basic rules for communication include the following: » Never take for granted that the receiver has the same reality as you. » Never take for granted that the receiver will interpret the message the way it was intended. » Communication is not an absolute, fi nite thing. » Always assume as many diff erent realities exist as there are diff erent people involved in the communication. Knowing these rules can greatly enhance the ability for good and useful communications. Th is is all good and great but what does communication have to do with developing a model? Even more, what does it have to do with social engineering?

**The Communication Model and Its Roots** As already established, communication basically means sending a packet of information to an intended receiver. Th e message may come from many sources like sight, sound, touch, smell, and words. Th is packet is then processed by the target and used to paint an overall picture of “What’s being said.” Th is method of assessment is called the communication process. Th is process was originally outlined by social scientists Claude Shannon and Warren Weaver in 1947, when they developed the Shannon-Weaver model, also known as “the mother of all models.” Th e Shannon-Weaver model, according to Wikipedia, “embodies the concepts of information source, message, transmitter, signal, channel, noise, receiver, information destination, probability of error, coding, decoding, information rate, [and] channel capacity,” among other things. Shannon and Weaver defi ned this model with a graphic, as shown in Figure 2-8. In a simple model, also known as the transmission model, information or content is sent in some form from a sender to a destination or receiver. Th is common concept of communication simply views communication as a means of sending and receiving information. Th e strengths of this model are its simplicity, generality, and quantifi ability. Shannon and Weaver structured this model based on: » An information source, which produces a message » A transmitter, which encodes the message into signals » A channel, to which signals are adapted for transmission » A receiver, which “decodes” (reconstructs) the message from the signal » A destination, where the message arrives Th ey argued that three levels of problems for communication existed within this theory: » Th e technical problem—How accurately can the message be transmitted? » Th e semantic problem—How precisely is the meaning conveyed? » Th e eff ectiveness problem—How eff ectively does the received meaning aff ect behavior? (Th is last point is important to remember for social engineering. Th e whole goal of the social engineer is to create a behavior that the social engineer wants.) Almost 15 years later, David Berlo expanded on Shannon and Weaver’s linear model of communication and created the Sender-Message-Channel-Receiver (SMCR) model of communication. SMCR separated the model into clear parts. Because the focus of this book is social engineers, you need to analyze what a social engineer can take away from all of this. After reading all this theory you may begin to wonder how this can be used. Remember, a social engineer must be a master at communication. They must be able to eff ectively enter into and remain in a person’s personal and mental space and not off end or turn off the target. Developing, implementing, and practicing eff ective communication models is the key to accomplishing this goal. Th e next step then is developing a communication model. You can think of communication as processes of information transmission governed by three levels of rules: » Formal properties of signs and symbols » Th e relations between signs/expressions and their users » Th e relationships between signs and symbols and what they represent Th erefore, you can further refi ne the defi nition of communication as social interaction where at least two interacting agents share a common set of signs and a common set of rules. In 2008 another researcher, D. C. Balmund, combined the research of many of his previous cohorts with his own and developed the transactional model of communication, as shown in Figure 2-10. In this model you can see that the channel and message can take on many forms, not just spoken, as represented by the picture. Th e message can be in written, video, or audio form and the receiver can be one person or many people. Th e feedback also can take on many forms. Combining and analyzing this research can help a social engineer develop a solid communication model. Not only social engineers can benefi t from doing this— everyone can. Learning how to develop a plan of communication can enhance the way you deal with your spouse, your kids, your employer or employees—anyone you communicate with.

**Developing a Communication Model** Now that you know about the key elements of a communication model, take a look at them from the eyes of a social engineer: » Th e Source: Th e social engineer is the source of the information or communication that is going to be relayed. » Th e Channel: Th is is the method of delivery. » Th e Message: Probably the biggest part of the message is knowing what you are going to say to the receiver(s). Feedback: What is your desired response? Th e desired response is to have the majority of the employees you send this email to click on it. Th at is ideal; of course, you might be happy with just a handful or even one, but the goal, the desired feedback, is to have the majority of targets click on the phishing link. » Receivers: Th is is where your information gathering skills come in handy. You need to know all about the targets. Do they like sports? Are they predominantly male or female? Are they members of local clubs? What do they do in their off time? Do they have families? Are they older or younger? Th e answers to these questions can help the social engineer decide what type of message to send. » Message: If the target is predominantly 25–40-year-old males, with a few being part of a fantasy football or basketball league, your targets may click on a link about sports, women, or a sporting event. Developing the email’s content is essential, but also grammar, spelling, and punctuation are very important to consider. One of the biggest tip-off s to phishing emails in the past has been the bad spelling. Getting an email that reads like this: “Click here and enter ur pasword to verify ur account settings,” is a dead giveaway to its being a non-legitimate email. Your email must be legit with good spelling and an appealing offer that fits the target. Even with the same goal the message will change depending on gender, age, and many other factors. The same email would probably fail if the targets were predominately female. » Channel: Th is answer to this element is easy, because you already know it is going to be an email. » Source: Again, this element is a no-brainer, because you, the social engineer, are the source. How believable you are depends on your skill level as a social engineer.

**The Power of Communication Models** Communication modeling is a powerful tool that is a must-have skill for every social engineer. Th e hardest part about communication modeling is to ensure your information-gathering sessions are solid. In both of the earlier scenarios, not having a good plan and model will lead to failure. A good way to practice communication modeling is to write out a model for manipulating people you know well—a husband, wife, parent, child, boss, or friend—to do something you want, to take some action you desire. Set a goal, nothing malicious, such as getting someone to agree to a diff erent vacation spot or a to go to a restaurant you love and your partner hates, or to allow you to spend some money on something you normally wouldn’t ask for. Whatever it is you come up with, write out the fi ve communication components and then see how well the communication goes when you have a written plan. You will fi nd that with your goals clearly defi ned, you can better test your social engineering communication methods, and be able to achieve your goals more easily. List the following fi ve points and fi ll them out one by one, connecting the dots as you go along. Communication modeling yields very valuable information and without it, most communication will not be successful for a social engineer. As previously mentioned, information gathering is the crux of every social engineering gig, but if you become profi cient at information gathering and you are able to gather amazing amounts of data but don’t know how to use it, it is a waste. Learn to become a master at information gathering and then practice putting that into action with communication modeling. Th is is just the start, but it can literally change the way you deal with people both as a social engineer and in everyday contexts. Yet so much more goes into developing a solid message in the communication model. One key aspect of learning how to communicate, how to manipulate, and how to be a social engineer is learning how to use questions, as discussed in the next chapter.

**Elicitation**

Being able to effectively draw people out is a skill that can make or break a social engineer. When people see you and talk to you they should feel at ease and want to open up. Have you ever met someone and instantly felt, “Wow I like that person”? Why? What was it about him that made you feel that way? Was it his smile? Th e way he looked? Th e way he treated you? His body language? Maybe he even seemed to be “in tune” with your thoughts and desires. Th e way he looked at you was non-judgmental and right away you felt at ease with him. Now imagine you can tap into that and master that ability. Don’t shrug off this chapter as a simple “how to build rapport” lesson. Th is chapter is about elicitation, a powerful technique used by spies, con men, and social engineers, as well as doctors, therapists, and law enforcement, and if you want to be protected or be a great social engineer auditor then you need to master this skill. Used eff ectively, elicitation can produce astounding results. What is elicitation? Very few aspects of social engineering are as powerful as elicitation. Th is is one of the reasons it is near the top of the framework. Th is skill alone can change the way people view you. From a social engineering standpoint, it can change the way you practice security. Th is chapter dissects examples of expert elicitation and delves deep into how to utilize this powerful skill in a social engineering context. Before getting in too deep, you must begin with the basics.

**What Is Elicitation?** Elicitation means to bring or draw out, or to arrive at a conclusion (truth, for instance) by logic. Alternatively, it is defi ned as a stimulation that calls up (or draws forth) a particular class of behaviors, as in “the elicitation of his testimony was not easy.” Read that defi nition again and if it doesn’t give you goose bumps you may have a problem. Th ink about what this means. Being able to eff ectively use elicitation means you can fashion questions that draw people out and stimulate them to take a path of a behavior you want. As a social engineer, what does this mean? Being eff ective at elicitation means you can fashion your words and your questions in such a way that it will enhance your skill level to a whole new level. In terms of information gathering, expert elicitation can translate into you target wanting to answer your every request. I want to take this discussion one step further because many governments educate and warn their employees against elicitation because it is used by spies all over the earth. In training materials, the National Security Agency of the United States government defi nes elicitation as “the subtle extraction of information during an apparently normal and innocent conversation.” Th ese conversations can occur anywhere that the target is—a restaurant, the gym, a daycare—anywhere. Elicitation works well because it is low risk and often very hard to detect. Most of the time, the targets don’t ever know where the information leak came from. Even if a suspicion exists that there is some wrong intent, one can easily pass it off as an angry stranger being accused of wrong doing for just asking a question. Elicitation works so well for several reasons: Most people have the desire to be polite, especially to strangers. Professionals want to appear well informed and intelligent. If you are praised, you will often talk more and divulge more. Most people would not lie for the sake of lying. Most people respond kindly to people who appear concerned about them. Th ese key factors about most humans are why elicitation works so well. Getting people to talk about their accomplishments is too easy. In one scenario in which I was tasked to gather intel on a company, I met my target at a local chamber of commerce function. Because it was a mixer I hung back until I saw the target approaching the bar. We got there at the same time and because the purpose of these functions is to meet and greet people and exchange business cards, my fi rst move wasn’t extreme. I said, “Escaping from the vultures?” He replied with a chuckle, “Yeah, this is what makes these things worth the time—open bar.” I listened to him order, and I ordered a similar drink. I lean over with my hand out, and said, “Paul Williams.” “Larry Smith.” I pulled out a business card I had ordered online. “I work with a little import company as the head of purchasing.” He said as he handed me his card, “I am the CFO for XYZ.” With a chuckle I responded, “You’re the guy with the bucks—that’s why everyone is after you out there. What exactly do you guys do?” He bagan to relate a few details of his company’s products, and when he listed one that is well known, I said, “Oh right, you guys make that widget; I love that thing. I read in XYZ Magazine it hit a new sales record for you guys.” From my previous information gathering I knew he had personal interest in that device so my praise was well received. He began to puff his chest out a bit. “Did you know that device sold more in the fi rst month that our previous and next fi ve products combined?” “Yikes, well I can see why, because I bought fi ve myself.” I chuckled through the mild praise. After another drink and some more time I was able to discover that they recently purchased accounting software, the name of the CSO (and the fact he was on vacation for a few days), and that my friend here was also going on vacation soon to the Bahamas with his wife. Th is seemingly useless info is not useless at all. I have a list of details about software, people, and vacations that can help me plan an attack. But I didn’t want to stop there; I went in for the kill with a question like this: “I know this is a weird question, but we are a small company and my boss told me I am to research and buy a security system for the doors. We just use keys now, but he was thinking RFID or something like that. Do you know what you guys use?” Th is question I thought would send up red fl ares and smoke signals. Instead, he said “I have no clue; I just signed the checks for it. What I do know is I have this fancy little card…” as he pulls out his wallet to show me his card. “I think it is RFID, but all I know is that I wave my wallet in front of the little box and the door opens.” We exchanged laughs and I walked away with knowledge that led to some very successful attack vectors. As you may have noticed, elicitation is similar to and linked to information gathering. Th is particular information-gathering session was made so much easier by a solid pretext (discussed in Chapter 4) as well good elicitation skills. Elicitation skills are what made the questions fl ow smoothly and what made the target feel comfortable answering my questions. Knowing that he was on vacation and what kinds of accounting software they used as well as the door locking security I was able to plan an onsite visit to repair a “faulty” RFID box and time clock. Simply telling the front desk receptionist, “Larry called me before he left for the Bahamas and said there was a time clock by the manufacturing department that is not registering properly. It will take me a few minutes to test and analyze it.” I was given access in a matter of seconds without ever being questioned. Elicitation led me to that success because with the knowledge I was given there was no reason for the receptionist to doubt my pretext. Simple, light, airy conversation is all it takes to get some of the best information out of many people. As discussed so far, clearly defi ning your goals to achieve maximum results is vital. Elicitation is not used merely for information gathering, but it can also be used to solidify your pretext and gain access to information. All of this depends on a clearly defi ned and thought-out elicitation model.

**The Goals of Elicitation** Reviewing the defi nition for elicitation can give you a clear path of what your goals are. Really, though, you can boil it down to one thing. A social engineer wants the target to take an action, whether that action be as simple as answering a question or as big as allowing access to a certain restricted area. To get the target to comply, the social engineer will ask a series of questions or hold a conversation that will motivate the target to that path. Information is the key. Th e more information that you gather, the more successful the attack will be. Because elicitation is non-threatening it is very successful. Count how many times in a week you have meaningless little conversations with someone at a store, coff ee shop, or elsewhere. Th e whole methodology of holding conversations is steeped in elicitation and it is used in a non-malicious way daily. That is why it is so eff ective. In one episode of the popular British television show Th e Real Hustle, the hosts demonstrated the ease of many social engineering attacks. In this episode the goal was to draw a target into a game of luck that was rigged. To do so someone had a partner who acted as a complete stranger play a role in being interested and conversational with the attacker. Th is conversation draws in the surrounding people, which made eliciting proper responses from the target very easy. Th is is one method that works well. Whichever method is used, the goal is to obtain information then utilize that information to motivate a target to the path the social engineer wants him to take. Understanding this fact is important. Later chapters cover pretexting and other manipulation tactics, but you don’t want to confuse elicitation with those. Realizing that elicitation is conversation is important. Sure, it may be closely linked to your pretext, body language, and eye cues, but all of those pale in comparison to your ability to engage people in conversation. Some experts agree that mastering the art of conversation has three main steps: 1. Be natural. Nothing can kill a conversation quicker than seeming to be uncomfortable or unnatural in the conversation. To see this for yourself try this exercise. Have a conversation with someone about something you know a lot about. If you can record it somehow or have someone else take notice, see how you stand, your posture, and the way you assert your knowledge. All of these things will scream confi dence and naturalness. Th en inject yourself in a conversation you know nothing about and have the same recording or friend observing. See how all those nonverbal aspects change for you when you try to inject an intelligent thought into a conversation you know nothing about. This exercise shows you the difference in being natural and not being natural. The person(s) you are conversing with will be able to see it easily, which will kill all chances of successful elicitation. How do you seem natural in conversations? Thus we arrive at step 2. 2. Educate yourself. You must have knowledge of what it is you will be talking to your targets about. Th is section should come with a big fat red neon light warning, but because every book can’t include one let me emphasize this part: It is imperative that you not pretend you are more than you can reasonably be believed you are. Confused? Here’s an example to break it down. If you wanted to obtain the chemical composition for a top-secret product and your elicitation target is one of the chemists involved in making the product, and you decide to start talking chemistry, do not play yourself off as a world-class chemist (unless you are). He may throw something at you that will show you know nothing and then your cover is blown and so is the elicitation. A more realistic approach may be that you are a research student studying XYZ, and was told he had amazing knowledge in this area. Due to his expertise, you just wanted to ask him a question on a chemical formula you are working on and why it doesn’t seem to be working out. The point is that whatever you chose to converse about and whomever with, do research, practice, and be prepared. Have enough knowledge to speak intelligently about a topic that will interest the target. 3. Don’t be greedy. Of course, the goal is to get information, get answers, and be given the key to the kingdom. Yet, do not let that be the focus. Th at you are only there for yourself will quickly become evident and the target will lose interest. Often, giving someone something will elicit the feeling of reciprocation (discussed in Chapter 6), where he or she now feels obligated to give you something in return. Being this way in conversation is important. Make the conversation a give and take, unless you are conversing with a person who wants to dominate the conversation. If he wants to dominate, let him. But if you get a few answers, feel the conversation out and don’t get greedy trying to go deeper and deeper, which can raise a red fl ag. Sometimes the people who are labeled as the “best conversationalists” in the world are those who do more listening than talking. Th ese three steps to successful elicitation can literally change the way you converse with people daily, and not just as a social engineer or a security auditor, but as an everyday person. I personally like to add one or two steps to the “top three.” For example, an important aspect to elicitation is facial expressions during a conversation. Having your gaze be too intense or too relaxed can aff ect the way people react to your questions. If your words are calm and you have engaged the target in a conversation but your body language or facial expressions show disinterest, it can aff ect the mood of the person, even if she doesn’t realize it. Th is may seem odd to bring up here, but I am a fan of Cesar Milan, aka, Th e Dog Whisperer. I think that guy is a genius. He takes dogs that seem unruly and in a matter of minutes has both the dogs and their owners produce high-quality personality traits that will merit a very successful relationship for both. He basically teaches people how to communicate with a dog—how to ask and tell it to do things in a language it understands. One of the things he preaches that I fully believe in is that the “spirit” or energy of the person aff ects the “spirit” or energy of the dog. In other words, if the person approaches the dog all tense and anxious, even if the words are calm, the dog will act tense, bark more, and be more on edge. Obviously, people are not the same as dogs but I truly believe that this philosophy applies. As a social engineer approaches a target her “spirit” or energy will aff ect the person’s perception. Th e energy is portrayed through body language, facial expressions, dress, and grooming, and then the words spoken to back that up. Without even knowing it, people pick up on these things. Have you ever thought or heard someone say, “Th at guy gave me the creeps” or “She looked like such a nice person”? How does that work? Th e person’s spirit or energy is relayed to your “sensors,” that data is correlated with past experiences, and then a judgment is formed. People do it instantaneously, many times without even knowing it. So your energy when you are going to elicit must match the role you are going to play. If your personality or mental makeup doesn’t enable you to easily play a manager then don’t try. Work with what you have. Personally, I have always been a people person and my strong suit is not topics like chemistry or advanced math. If I were in the situation mentioned earlier I would not try to play the role of a person who knows about those things. Instead my elicitation might be as simple as a stranger interested in starting a conversation about the weather. Whatever methods you chose to use, you can take certain steps to have the upper edge. One of these steps is called preloading. You stand in line to buy your $10 movie ticket and are barraged with sensory overload of posters of upcoming movies. You stand in line to buy your $40 worth of popcorn and drinks, see more posters, and then you push your way through to get a seat. Finally, when the movie starts you are presented with a series of clips about upcoming movies. Sometimes these movies aren’t even in production yet, but the announcer comes on and says, “Th e funniest movie since…” or the music starts with an ominous tone, a dense fog fi lls the screen, and the voiceover intones, “You thought it was over in Teenage Killer Part 45….” Whatever the movie is, the marketers are telling you how to feel—in other words, preloading what you should be thinking about this movie—before the preview starts. Th en the short 1–3 minutes they have to show you what the movie is about is spent showing you clips to entice your desire to see the movie and to appeal to the crowd that wants the comedy, horror, or love story. Not much has been written about preloading, but it is a very serious topic. Preloading denotes that you can do just what it says—preload targets with information or ideas on how you want them to react to certain information. Preloading is often used in marketing messages; for example, in the national restaurant chain ads that show beautiful people laughing and enjoying the meal that looks so beautiful and perfect. As they say “yummm!” and “ohhh!” you can almost taste the food. Of course as a social engineer you can’t run a commercial for your targets so how can you use preloading? As with much in the social engineering world, you have to start from the end results and work backward. What is your goal? You might have the standard goal of elicitation to gain information from a target on a project she is working on or dates she will be in the offi ce or on vacation. Whatever it is, you must set the goal fi rst. Next you decide the type of questions that you want to ask, and then decide what type of information can preload a person to want to answer those questions. For example, if you know that later tonight you want to go to a steak place that your coupon-loving wife doesn’t really enjoy, but you are in the mood for a rib eye, you can preload to get a response that may be in your favor. Maybe earlier in the day you can say something like, “Honey, you know what I am in the mood for? A big, juicy, grilled steak. Th e other day I was driving to the post offi ce and Fred down the road had his grill out. He had just started cooking the steaks on charcoal and the smell came in the car window and it has been haunting me ever since.” Whether this elicits a response at this exact moment is not important; what you did is plant a seed that touched every sense. You made her imagine the steaks sizzling on the grill, talked about seeing them go on, talked about smelling the smoke, and about how much you wanted one. Suppose then you bring home the paper and as you’re going through it you see an ad with a coupon for the restaurant you want to go to. You simply leave that page folded on the table. Again, maybe your wife sees it or maybe she doesn’t, but chances are that because you left it with the mail, because you mentioned steak, and because she loves coupons she will see the coupon left on the table. Now later on she comes to you and says, “What do you want for dinner tonight?” Here is where all your preloading comes in—you mentioned the smell, sight, and desire for steak. You left an easy-to-fi nd coupon on the table for the steak restaurant of choice and now it is dinner discussion time. You answer her with, “Instead of making you cook and having a mess to clean up tonight, we haven’t been to XYZ Steaks in a while. What if we just hit that place tonight?” Knowing she doesn’t like that place all you can hope is the preloading is working. She responds, “I saw a coupon for that place in the newspaper. It had a buy one meal get a second half off . But you know I don’t like….” As she is speaking you can jump in and off er praise: “Ha! Coupon queen strikes again. Heck, I know you don’t like steak too much but I hear from Sally that they have awesome chicken meals there, too.” A few minutes later you are on the way to steak heaven. Whereas a frontal assault stating your desire to go to XYZ would have most likely met with a resounding “No!” preloading helped set her mind up to accept your input and it worked. One other really simplistic example before moving on: A friend walks up and says, “I have to tell you a really funny story.” What happens to you? You might even start smiling before the story starts and your anticipation is to hear something funny, so you look and wait for opportunities to laugh. He preloaded you and you anticipated the humor. How do these principles work within the social engineering world? Preloading is a skill in itself. Being able to plant ideas or thoughts in a way that is not obvious or overbearing sometimes takes more skill than the elicitation itself. Other times, depending on the goal, preloading can be quite complex. Th e earlier steak scenario is a complex problem. Th e preload took some time and energy, where a simplistic preload might be something as simple as fi nding out what kind of car they drive or some other innocuous piece of information. In a very casual conversation where you “happen” to be in the same deli at the same time as your target you start a casual conversation with something like, “Man, I love my Toyota. Th is guy in a Chevy just backed into me in the parking lot, not even a scratch.” With any luck as you engage the target in conversation, your exclamation about your car might warm him up to the questions that you can then place about types of cars or other topics you want to gather intel on. Th e topic of preloading makes more sense as you start to analyze how you can utilize elicitation. Social engineers have been mastering this skill for as long as social engineering has been around. Many times the social engineer realizes he has this skill way before he turns to a life of social engineering. As a youth or a young adult he fi nds interacting with people easy, and later fi nds that he gravitates toward employment that uses these skills. Maybe he is the center of his group of friends and people seem to tell him all their problems and have no problem talking to him about everything. He realizes later that these skills are what gets him through doors that might be closed otherwise. When I was young I always had this talent. My parents would tell me stories of how I at fi ve or six years old would strike up conversations with complete strangers, sometimes even walking into the kitchen of busy restaurants to ask questions about our order or inquire how things were being done. Somehow I got away with it—why? Probably because I didn’t know this behavior wasn’t acceptable and because I did it with confi dence. As I got older, that skill (or a lack of fear) came into full eff ect. It also seemed that people, sometimes even complete strangers, loved to tell me their problems and talk to me about things. One story that I think helps to see how I was able to utilize not only preloading but also good elicitation skills was when I was around 17 or 18 years old. I was an avid surfer and would do odd jobs to support my hobby—basically anything from pizza delivery to fi berglass cutter to lifeguard. One time I ran errands for my father who owned an accounting/fi nancial consulting company. I would deliver papers to his clients, get signatures, and bring them back. Often, many of the clients would open up and tell me all about their lives, their divorces, and their business successes and failures. Usually this started with a small session with them telling me how great my Dad was to them. At the time I never understood why people, especially adults, would open up to a 17–18 year old with the reasons their universe is breaking apart. One particular client I would visit often owned an apartment complex. It was nothing huge and fancy; he just had a few properties that he owned and managed. Th is poor guy had real problems—family problems, health problems, and personal problems—all of which he routinely would tell me about for as long as I would sit and listen. Th is is when it began to hit me that I could get away with saying or doing amazing things if I just spent time listening to people. It made them feel important and like I was a good person. It didn’t matter if I sat there thinking about my next great wave; what mattered was that I listened. Normally I would listen for as long as I could stand the amazing amount of tobacco smoke he put out (he smoked more than any person I ever have seen in my life). But I would sit and listen and because I was young and had no experience I would off er no advice, no solution, just an ear. Th e thing was that I was truly concerned; I didn’t fake it. I wished I had a solution. One day he told me about how he wanted to move back out West where his daughter was and be closer to family. I wanted to move on in life and get a job I thought would be cool, fun, and give me some more cash for surfboards and other things I “needed.” During one of my listening sessions, a crazy idea popped in my head, and he viewed me as a responsible, compassionate young man with a “good head” on my shoulders. Th e preloading took place over the months I spent sitting with him and listening. Now it was time to cash in on that. I said, “Why don’t you go back and let me run your apartment complex for you?” Th e idea was so absurd, so ridiculous that looking back now I would have laughed in my face. But for weeks, months even, I had listened to his problems. I knew the man and his woes. On top of that, I never laughed at or rejected him. Now he had shared a problem with me, and here was a perfect solution, one that took care of all of his problems as well as mine. My income needs were low, and he wanted to be close to his family. We had built a relationship over the last few months and thus he “knew” me and trusted me. After some discussion we came to an agreement and he up and moved back out West and I was a 17-year-old running a 30-unit apartment complex as the vicelandlord. I could go on and tell you much more on this story but the point is already made. (I will tell you the job went great until he asked me to try to sell his complex for him, which I did in record time, at the same time selling myself out of a job.) Th e point is that I developed a rapport, a trust, with someone and without trying and without malicious intent, I had a chance to preload him over months with the ideas that I was kind and compassionate and intelligent. Th en when the time arose I was able to present an absurd idea, and because of the months of preloading, it was accepted. It wasn’t until later in life that it hit me what was going on here. Th ere were so many factors at play that I didn’t realize at the time. Preloading from a social engineering standpoint involves knowing your goal before you start. In this case, I didn’t know I was going to try and land a crazy job with this guy. But preloading still worked. In most social engineering cases it would much quicker, but I think the principles apply. Being as genuine as you can is essential. Because preloading involves the person’s emotions and senses, give them no reason to doubt. Th e question you ask should match your pretext. For preloading to work you have to ask for something that matches the belief you built into them. For example, if my off er was to have me go visit my client’s family and take pictures rather than manage his apartment complex, it wouldn’t have matched the belief system he had of me, namely that I was a smart, business-minded, caring young man. Finally, the off er, when made, must be of benefi t to the target, or at least perceived as benefi t. In my case, there was lots of benefi t to my client. But in social engineering the benefi t can be as little as “bragging rights”: giving the person a platform to brag a bit. Or the benefi t can be much more and involve physical, monetary, or psychological benefi ts. Practicing elicitation and becoming profi cient at it will make you a master social engineer. Logically, the next section is how to become a successful elicitor.

**Becoming a Successful Elicitor** Analyzing just my own experiences I can identify some key components that led to my success from fi ve-years-old to now: » A lack of fear to talk to people and be in situations that are not considered “normal.” » I truly do care for people, even if I don’t know them. I want to and enjoy listening to people. » I off er advice or help only when I have a real solution. » I off er a non-judgmental ear for people to talk about their problems. Th ese are key elements to successful elicitation. Th e United States Department of Homeland Security (DHS) has an internal pamphlet on elicitation it hands out to its agents that I was able to obtain and archive at www.social-engineer.org/ wiki/archives/BlogPosts/ocso-elicitation-brochure.pdf. Th is brochure contains some excellent pointers. Basically, as stated in it and in this chapter, elicitation is used because it works, is very hard to detect, and is non-threatening. Th e DHS pamphlet approaches elicitation from a “how to avoid” point of view, but the following sections take some of the scenarios and show you what can be learned.

**Appealing to Someone’s Ego** Th e scenario painted in the DHS brochure goes like this: Attacker: “You must have an important job; so and so seems to think very highly of you.” Target: “Th ank you, that is nice of you to say, but my job isn’t that important. All I do here is…” Th e method of appealing to someone’s ego is simplistic but eff ective. One caution, though: Stroking someone’s ego is a powerful tool but if you overdo it or do it without sincerity it just turns people off . You don’t want to come off as a crazy stalker: “Wow, you are the most important person in the universe and you are so amazing-looking, too.” Saying something like that might get security called on you. Using ego appeals needs to be done subtly, and if you are talking to a true narcissist avoid eye rolls, sighs, or argumentativeness when she brags of her accomplishments. Subtle ego appeals are things like, “Th at research you did really changed a lot of people’s viewpoints on…” or “I overheard Mr. Smith telling that group over there that you are one of the most keen data analysts he has.” Don’t make the approach so over the top that it is obvious. Subtle fl attery can coax a person into a conversation that might have never taken place, as stated in the DHS brochure, and that is exactly what you want as a social engineer.

**Expressing a Mutual Interest** Consider this mock scenario: Attacker: “Wow, you have a background in ISO 9001 compliance databases? You should see the model we built for a reporting engine to assist with that certifi cation. I can get you a copy.” Target: “I would love to see that. We have been toying with the idea of adding a reporting engine to our system.” Expressing mutual interest is an important aspect of elicitation. Th is particular scenario is even more powerful than appealing to someone’s ego because it extends the relationship beyond the initial conversation. Th e target agreed to further contact, to accept software from the attacker, and expressed interest in discussing plans for the company’s software in the future. All of this can lead to a massive breach in security. Th e danger in this situation is that now the attacker has full control. He controls the next steps, what information is sent, how much, and when it is released. Th is is a very powerful move for the social engineer. Of course, if the engagement were long-term, then having a literal piece of software that can be shared would prove even more advantageous. Sharing usable and non-malicious software would build trust, build rapport, and make the target have a sense of obligation.

**Making a Deliberate False Statement** Delivering a false statement seems like it would backfi re off the top, but it can prove to be a powerful force to be reckoned with. Attacker: “Everybody knows that XYZ Company produced the highest-selling software for this widget on earth.” Target: “Actually, that isn’t true. Our company started selling a similar product in 1998 and our sales records have beaten them routinely by more than 23%.” Th ese statements, if used eff ectively, can elicit a response from the target with real facts. Most people must correct wrong statements when they hear them. It’s almost as if they are challenged to prove they are correct. Th e desire to inform others, appear knowledgeable, and be intolerant of misstatements seems to be built into human nature. Understanding this trait can make this scenario a powerful one. You can use this method to pull out full details from the target about real facts and also to discern who in a group might have the most knowledge about a topic.

**Volunteering Information** The DHS brochure makes a good point about a personality trait many of us have. A few mentions of it have appeared in the book already and it’s covered in much more detail later on, but obligation is a strong force. As a social engineer, off ering up information in a conversation almost compels the target to reply with equally useful information. Want to try this one out? Next time you are with your friends say something like, “Did you hear about Ruth? I heard she just got laid off from work and is having serious problems fi nding more work.” Most of the time you will get, “Wow, I didn’t hear that. Th at is terrible news. I heard that Joe is getting divorced and they are going to lose the house, too.” A sad aspect of humanity is that we tend to live the saying “misery loves company”—how true it is in this case. People tend to want to share similar news. Social engineers can utilize this proclivity to set the tone or mood of a conversation and build a sense of obligation.

**Assuming Knowledge** Another powerful manipulation tool is that of assumed knowledge. It is commonplace to assume that if someone has knowledge of a particular situation, it’s acceptable to discuss it with them. An attacker can deliberately exploit this trait by presenting information as if he is in the know and then using elicitation to build a conversation around it. He then can regurgitate the information as if it were his own and continue to build the illusion that he has intimate knowledge of this topic. Th is scenario might be better illustrated with an example. One time I was going to China to negotiate a large deal on some materials. I needed to have some intimate knowledge about my target company in the negotiations and had to fi nd a way to get it before I met with them. We had never met face to face but I was heading to a conference in China before my negotiations started. While at the conference I happened to overhear a conversation starting about how to place yourself in a higher position when dealing with the Chinese on negotiations. I knew this was my opportunity, and to make the situation even sweeter one of the people in the small group was from the company I was going to be meeting with. I quickly injected myself into the conversation and knew that if I didn’t say something quick I would lose face. My knowledge was limited but they didn’t need to know that. When a small pause arose I began to talk about the Guanxi theory. Guanxi is basically how two people who may not have the same social status can become connected, and then one is pressed upon to perform a favor for the other. I talked about how this connection can be used, and then concluded by tying it in with how important it is as an American to not simply take a business card and stick it in my back pocket but to review it, comment on it, then place it somewhere respectful. Th is conversation was enough to set me up as someone who had some knowledge and deserved to stay in the circle of trust there. Now that I had established my knowledge base I sat back and listened to each person express his or her experience and personal knowledge on how to negotiate properly with large Chinese companies. I paid very close and particular attention when the gentlemen who worked for my target company spoke. As he talked I could tell the “tips” he was giving were closely linked to the business philosophies of his company. Th is knowledge was more valuable than anything I could have paid for and it led to a very successful trip. Th ere are a couple more scenarios I feel are often used in elicitations.

**Using the Effects of Alcohol** Nothing loosens lips more than the juice. Th is is an unfortunate but true fact. Mix any one of the preceding fi ve scenarios with alcohol and you can magnify its eff ects by 10. Probably the best way to describe this scenario is with a true story. In 1980 a senior scientist from Los Alamos National Laboratory traveled to a research institute in the People’s Republic of China (PRC) to talk about his specialty, nuclear fusion. He had extensive knowledge of U.S. nuclear weapons information but knew the situation he was entering was dangerous and he needed to be determined to stick to his topic. Yet he was constantly barraged with increasingly detailed inquiries directly related to nuclear weapons. Th e attackers’ tactics would change and they would ask many benign questions about fusion and astrophysics, his specialty. Once they even threw a cocktail party in his honor. Th ey gathered around and applauded his knowledge and research—each time with a toast and a drink. Th ey began to inquire about classifi ed matters such as the ignition conditions of deuterium and tritium, the two components in the then-new neutron bomb. He did well at fending off the constant questions, but after many toasts and a party in his honor, he decided to give an analogy. He mused to the group that if you rolled those two components into a ball and then rolled them off the table they would most likely ignite because they had such low temperature threshold levels. Th is seemingly useless story and information most likely caused the researchers in China to discern a clear path of research on nuclear weapons. Th ey would take this information to yet another scientist and now armed with a little more knowledge, use that knowledge to get to the next stage with him or her. After many attempts, it is very likely the Chinese scientist would possess a clear picture of what path to take. Th is is a serious example of how using elicitation can lead to gaining a clear picture of the whole answer. In social engineering it may be the same for you. All the answers might not come from one source. You may elicit some information from one person about their whereabouts on a particular date, and then use that information to elicit more information from the next stage, and so on and so forth. Putting those nuggets of information together is often the hard part of perfecting elicitation skills. Th at is discussed next.

**Using Intelligent Questions** As a social engineer you must realize that the goal with elicitation is not to walk up and say, “What is the password to your servers?” Th e goal is getting small and seemingly useless bits of information that help build a clear picture of the answers you are seeking or the path to gaining those answers. Either way, this type of information gathering can help give the social engineer a very clear path to the target goal. How do you know what type of questions to use? Th e following sections analyze the types of questions that exist and how a social engineer can use them.

**Open-Ended Questions** Open-ended questions cannot be answered with yes or no. Asking, “Pretty cold out today, huh?” will lead to a “Yes,” “Uh-uh,” “Yep,” or some other similar affirmative guttural utterance, whereas asking, “What do you think of the weather today?” will elicit a real response: the person must answer with more than a yes or no. One way a social engineer can learn about how to use open-ended questions is to analyze and study good reporters. A good reporter must use open-ended questions to continue eliciting responses from his or her interviewee. Suppose I had plans to meet a friend and he canceled, and I wanted to know why. I can ask a question like, “I was curious about what happened to our plans the other night.” “I wasn’t feeling too well.” “Oh, I hope you are better now. What was wrong?” Th is line of questioning usually gets more results than doing an all-out assault on the person and saying something like, “What the heck, man? You ditched me the other night!” Another aspect of open-ended questions that adds power is the use of why and how. Following up a question with how or why can lead to a much more in-depth explanation of what you were originally asking. Th is question again is not “yes” or “no” answerable, and the person will reveal other details you may fi nd interesting. Sometimes open-ended questions can meet with some resistance, so using the pyramid approach might be good. Th e pyramid approach is where you start with narrow questions and then ask broader questions at the end of the line of questioning. If you really want to get great at this technique learn to use it with teenagers. For example, many times open-ended questions such as, “How was school today?” will be met with an “OK” and nothing more, so asking a narrow question might open up the fl ow of information better. “What are you doing in math this year?” Th is question is very narrow and can be answered only with a very specifi c answer: “Algebra II.” “Ah, I always hated that. How do you like it?” From there you can always branch out into broader questions, and after you get the target talking, getting more info generally becomes easier.

**Closed-Ended Questions** Obviously, closed-ended questions are the opposite of open-ended questions but are a very eff ective way to lead a target where you want. Closed-ended questions often cannot be answered with more than one or two possibilities. In an open-ended question one might ask, “What is your relationship with your manager?” but a closed-ended question might be worded, “Is your relationship with your manager good?” Detailed information is usually not the goal with closed-ended questions; rather, leading the target is the goal. Law enforcement and attorneys use this type of reasoning often. If they want to lead their target down a particular path they ask very closed questions that do not allow for freedom of answers. Something like this: “Do you know the defendant, Mr. Smith?” “Yes I do.” “On the night of June 14th, did you see Mr. Smith at the ABC Tavern?” “I did.” “And at what time was that?” “11:45pm.” All of these questions are very closed ended and only allow for one or two types of responses.

**Leading Questions** Combining aspects from both open- and closed-ended questions, leading questions are open ended with a hint leading toward the answer. Something like, “You were at the ABC Tavern with Mr. Smith on June 14th at around 11:45pm, weren’t you?” Th is type of question leads the target where you want but also off ers him the opportunity to express his views, but very narrowly. It also preloads the target with the idea that you have knowledge of the events being asked about. Leading questions often can be answered with a yes or no but are diff erent from closed-ended questions because more information is planted in the question that when answered gives the social engineer more information to work with. Leading questions state some facts and then ask the target to agree or disagree with them. In 1932 the British psychologist Frederic C. Bartlett concluded a study on reconstructive memory. He told subjects a story and then asked them to recall the facts immediately, two weeks later, and then four weeks later. Bartlett found that subjects modifi ed the story based on their culture and beliefs as well as personality. None were able to recall the story accurately and in its entirety. It was determined that memories are not accurate records of our past. It seems that humans try to make the memory fi t into our existing representations of the world. When asked questions, many times we respond from memory based on our perceptions and what is important to us. Because of this, asking people a leading question and manipulating their memory is possible. Elizabeth Loftus, a leading fi gure in the fi eld of eyewitness testimony research, has demonstrated through the use of leading questions how distorting a person’s memory of an event is easily possible. For example, if you showed a person a picture of a child’s room that contained no teddy bear, and then asked her, “Did you see a teddy bear?” you are not implying that one was in the room, and the person is free to answer yes or no as they wish. However, asking, “Did you see the teddy bear?” implies that one was in the room and the person is more likely to answer “yes,” because the presence of a teddy bear is consistent with that person’s schema of a child’s room. Because of this research the use of leading questions can be a powerful tool in the hands of a skilled social engineer. Learning how to lead the target can also enhance a social engineer’s ability to gather information.

**Assumptive Questions** Assumptive questions are just what they sound like—where you assume that certain knowledge is already in the possession of the target. Th e way a social engineer can determine whether or not a target possesses the information he is after is by asking an assumptive question. For example, one skill employed by law enforcement is to assume the target already has knowledge—for example, of a person—and ask something like, “Where does Mr. Smith live?” Depending on the answer given, the offi cer can determine whether the target knows the person and how much she knows about him. A good point to note is that when a social engineer uses assumptive questions the whole picture should never be given to the target. Doing so gives all the power to the target and removes much of the social engineer’s ability to control the environment. Th e social engineer never wants to use assumptive questions to accuse the target of a wrong. Doing so alienates the target and again costs the social engineer power. A social engineer should use assumptive questions when he has some idea of the real facts he can use in the question. Using an assumptive question with bogus information may turn the target off and will only confi rm that the target doesn’t know about something that didn’t happen. Back to an earlier example, if I wanted to gain information from a leading chemist and I did some research and knew enough to formulate one intelligent sentence I could make an assumptive question but it would ruin future follow up if I was not able to back up the assumption the target would make of my knowledge. For example, if I were to ask, “Because deuterium and tritium have such low temperature thresholds, how does one handle these materials to avoid ignition?” Th e follow-up information might be hard to follow if I am not a nuclear physicist. Th is is counterproductive and not too useful. Plan your assumptive questions to have the maximum eff ect. One adjunct that is taught to law enforcement offi cials that comes in very handy when using assumptive questions is to say, “Now think carefully before you answer the next question…” Th is kind of a statement preloads the target’s mind with the idea that he must be truthful with his next statement. It can take months or years to master these skills. Don’t get disheartened if the fi rst few attempts are not successful, and keep trying. Don’t fear, though, there are some tips to mastering this skill. I will review these in closing.

**Mastering Elicitation** Th is chapter has a lot of information for you to absorb, and if you are not a people person, employing the techniques covered might seem like a daunting task. Like most aspects of social engineering, elicitation has a set of principles that when applied will enhance your skill level. To help you master these principles, remember these pointers: Too many questions can shut down the target. Peppering the target with a barrage of questions will do nothing but turn off the target. Remember, conversation is a give and take. You want to ask, but you have to give to make the target feel at ease. Too few questions will make the target feel uncomfortable. Have you ever been in a conversation that is fi lled with “awkward silences”? It isn’t good is it? Don’t assume that your target is a skilled and willing conversationalist. You must work at making a conversation an enjoyable experience. Ask only one question at a time. Chapter 5 covers buff er overfl ows on the human mind, but at this time your goal is not to overfl ow the target. It is to merely gather information and build a profi le. To do this you can’t seem too eager or non-interested. As you have probably gathered, making elicitation work right is a delicate balance. Too much, too little, too much at once, not enough—any one of them will kill your chances at success. However, these principles can help you master this amazing talent. Whether you use this method for social engineering or just learning how to interact with people, try this: Th ink of conversation as a funnel, where on the top is the largest, most “neutral” part and at the bottom is the very narrow, direct ending. Start by asking the target very neutral questions, and gather some intel using these questions. Give and take in your conversation, and then move to a few openended questions. If needed, use a few closed-ended questions to direct the target to where you want to go and then if the situation fi ts, move to highly directed questions as you reach the end of funnel. What will pour out of the “spout” of that funnel is a river of information. Th ink about it in the situation discussed in this chapter of my target at the chamber of commerce gathering. My goal was to gather intel on anything that might lead to a security breach. I started off the conversation with a very neutral question. “Escaping the vultures?” Th is question broke the ice on the conversation as well as used a little humor to create a bridge that allowed us to exist on the same plane of thought. I asked a few more neutral questions and handed him my card while inquiring what he does. Th is segues smoothly into the open-ended questions. A brief information-gathering session that occurred earlier, using carefully placed closed-ended or assumptive questions was key. After hearing about the company’s recent purchase for new accounting software and network upgrades I wanted to go in for the kill. Having scoped out the building I knew it used RFID, but I wasn’t sure if the target would go so far as to describe the card and show it to me. Th is is where the use of direct questions played a role: coming right out and asking what security the company used. By the time I used that type of question our rapport and trust factor was so high he probably would have answered any questions I asked. Understanding how to communicate with people is an essential skill for an elicitor. Th e social engineer must be adaptive and able to match the conversation to his or her environment and situation. Quickly building even the smallest amount of trust with the target is crucial. Without that rapport, the conversation will most likely fail. Other key factors include making sure that your communication style, the questions used, and the manner in which you speak all match your pretext. Knowing how to ask questions that force a response is a key to successful elicitation, but if all that skill and all those questions do not match your pretext then the elicitation attempt will most surely fail.

**How to become anyone**

At times we probably all wish we could be someone else. Heck, I would love to be a little skinnier and better looking. Even though medical science hasn’t come up with a pill that can make that possible, a solution to this dilemma does exist—it’s called pretexting. What is pretexting? Some people say it is just a story or lie that you will act out during a social engineering engagement, but that defi nition is very limiting. Pretexting is better defi ned as the background story, dress, grooming, personality, and attitude that make up the character you will be for the social engineering audit. Pretexting encompasses everything you would imagine that person to be. Th e more solid the pretext, the more believable you will be as a social engineer. Often, the simpler your pretext, the better off you are. Pretexting, especially since the advent of the Internet, has seen an increase in malicious uses. I once saw a t-shirt that read, “Th e Internet: Where men are men, women are men, and children are FBI agents waiting to get you.” As slightly humorous as that saying is, it has a lot of truth in it. On the Internet you can be anyone you want to be. Malicious hackers have been using this ability to their advantage for years and not just with the Internet. In social engineering playing a role or being a diff erent person to successfully accomplish the goal is often imperative. Chris Hadnagy might not have as much pull as the tech support guy or the CEO of a major importing organization. When a social engineering situation arises, having the skills needed to become the pretext is important. In a discussion I was having with world-renowned social engineer Chris Nickerson, on this topic, he said something I think really hits home. Nickerson stated that pretexting is not about acting out a role or playing a part. He said it is not about living a lie, but actually becoming that person. You are, in every fi ber of your being, the person you are portraying. Th e way he walks, the way he talks, body language—you become that person. I agree with this philosophy on pretexting. Often when people watch a movie the ones we feel are the “best we have ever seen” are where the actors get us so enthralled with their parts we can’t separate them from their portrayed characters. Th is was proven true to me when many years ago my wife and I watched a great movie with Brad Pitt, Legends of the Fall. He was a selfi sh jerk in this movie, a tormented soul who made a lot of bad decisions. He was so good at playing this part my wife literally hated him as an actor for a few years. Th at is a good pretexter. Th e problem with using pretexting for many social engineers is that they feel it is just dressing up as a part and that’s it. True, the dress can help, but pretexting is a science. In a way, your whole persona is going to portray you in a light that is diff erent than who you are. To do this, you, as a social engineer, must have a clear picture of what pretexting really is. Th en you can plan out and perform the pretext perfectly. Finally, you can apply the fi nishing touches. Th is chapter will cover those aspects of pretexting. First is a discussion of what pretexting really is. Following that is discussion of how to use pretexting as a social engineer. Finally, to tie it all together, this chapter explores some stories that show how to use pretexting eff ectively. Pretexting is defi ned as the act of creating an invented scenario to persuade a targeted victim to release information or perform some action. It is more than just creating a lie; in some cases it can be creating a whole new identity and then using that identity to manipulate the receipt of information. Social engineers can use pretexting to impersonate people in certain jobs and roles that they never themselves have done. Pretexting is not a one-size-fi ts-all solution. A social engineer must develop many diff erent pretexts over his or her career. All of them will have one thing in common: research. Good information gathering techniques can make or break a good pretext. For example, mimicking the perfect tech support rep is useless if your target does not use outside support. Pretexting is also used in areas of life other than social engineering. Sales; public speaking; so-called fortune tellers; neurolinguistic programming (NLP) experts; and even doctors, lawyers, therapists, and the like all have to use a form of pretexting. Th ey all have to create a scenario where people are comfortable with releasing information they normally would not. Th e diff erence in social engineers using pretexting and others is the goals involved. A social engineer, again, must live that persona for a time, not just act a part. As long as the audit or social engineering gig lasts, you need to be in the persona. I “get in character” myself, as do many of my colleagues, some of whom even stay in character “off the clock.” Anywhere you need to, you should be the pretext you set out to be. In addition, many professional social engineers have many diff erent online, social media, email, and other accounts to back up a slew of pretexts. I once interviewed radio icon Tom Mischke on this topic for a social engineering podcast I am a part of (hosted at www.social-engineer.org/episode-002- pretexting-not-just-for-social-engineers/). Radio hosts must be profi cient at pretexting because they constantly have to release only the information they want to the public. Tom was so profi cient at this that many listeners felt as if they “knew” him as a friend. He would get invitations to weddings, anniversaries, and even births. How was Tom able to accomplish this amazing kind of pretext? Th e answer is practice. Lots and lots of practice is what he prescribed. He told me that he would actually plan out his “acts” then practice them—use the voice they would have, sit how they would sit, maybe even dress like they would dress. Practice is exactly what makes a good pretext. A very important aspect to remember is that the quality of the pretext is directly linked to the quality of the information gathered. Th e more, the better, and the more relevant the information the easier it will be for the pretext to be developed and be successful. For example, the classic pretext of a tech support guy would utterly fail if you went to a company that either had internal support or outsourced to a very small company of one or two people. As natural as you are when you converse with someone about who you really are is how easy applying your pretext should be. So that you can see how you can utilize this skill, the following section covers the principles of pretexting then shows how you can apply them to actually planning a solid pretext.

**The Principles and Planning Stages of  Pretexting** As with every skill, certain principles dictate the steps to performing that task. Pretexting is no diff erent. Th e following is a list of principles of pretexting that you can use. By no means are these the only principles out there; maybe others can be added, but these principles embody the essence of pretexting: The more research you do the better the chance of success. Involving your own personal interests will increase success. Practice dialects or expressions. Many times social engineering eff ort can be reduced if the phone is viewed as less important. But as a social engineer, using the phone should not reduce the eff ort put into the social engineering gig Th e simpler the pretext the better the chance of success. Th e pretext should appear spontaneous. Provide a logical conclusion or follow through for the target.

**The More Research You Do, the Better the Chance of Success** This principle is self-explanatory, but it can’t be said enough—the level of success is directly connected to the level and depth of research. As discussed in Chapter 2, it is the crux of successful social engineering. Th e more information a social engineer holds the more chances he or she has of developing a pretext that works. Remember the story I told in Chapter 2 about my mentor Mati Aharoni and how he convinced a high-level executive to visit his “stamp collection” site online? At fi rst glance, the path inside that company might have seemed to be something to do with fi nancial, banking, fund raising, or something along those lines because it was a banking facility. Th e more research Mati did, the clearer it became that the pretext could be a person who was selling a stamp collection. Finding out what the executive’s interests were allowed Mati to fi nd an easy way into the company, and it worked. Sometimes those little details that are what make the diff erence. Remember, no information is irrelevant. While gathering information, looking for stories, items, or aspects of a personal nature is also a good idea. Using a target’s personal or emotional attachments can enable you to get a foot in the door. If the social engineer fi nds out that every year the CFO donates a sizable sum to a children’s cancer research center, then a pretext that involves fund raising for this cause could very likely work, as heartless as it sounds. Th e problem is that malicious social engineers use pretexts that feed on emotions without a second thought. After the attacks on the Twin Towers in New York City on September 11, 2001, many malicious hackers and social engineers used the losses of these people to raise funds for themselves via websites and emails that targeted people’s computers and fake fund raisers that obtained funds from those with a giving heart. After the earthquakes in Chile and Haiti in 2010, the same things occurred where many malicious social engineers developed websites that were positioned as giving out information on the seismic activity or the people who were lost. Th ese sites were encoded with malicious code and hacked people’s computers. Th is is even more evident directly after the death of a movie or music star. Search engine optimization (SEO) and marketing geniuses will have the search engines pulling up their stories in a matter of hours. Along with marketers, malicious social engineers will take advantage of the increased search engine attention by launching malicious sites that feed off that SEO. Drawing people to these sites, they harvest information or infect them with viruses. Th at people will take advantage of others’ misfortune is a sad fact about this world, and one of those dark corners I said you would visit in this book. As a social engineering auditor, I can use an employee’s emotions to show a company that even people with seemingly good intentions can trick a company’s employees into giving access to valuable and business-ruining data. All these examples solidify the point that the better a social engineer’s information-gathering and research-gathering process, the better chance he has at fi nding some detail that will increase the chances of a successful pretext.

**Involve Personal Interests to Increase Success** Using your own personal interests to increase the chances of a successful social engineering move seems very simple but it can go a long way in convincing the target that you are credible. Nothing can ruin rapport and trust faster than a person who claims to be knowledgeable about a topic and then falls short. As a social engineer, if you have never seen a server room before and have never taken a computer apart, trying to play the part of a technician can be a quick path to failure. Including topics and activities in your pretext that you are interested in gives you a lot to talk about and gives you the ability to portray intelligence as well as confi dence. Confi dence can go a long way toward convincing the target you are who you say you are. Certain pretexts require more knowledge than others (for instance, stamp collector versus nuclear researcher) to be convincing, so again research becomes the recurring theme. Sometimes the pretext is simple enough that you can get the knowledge by reading a few websites or a book. However you gain the knowledge, researching topics that personally interest you, as the social engineer, is important. After you pick up on a story, aspect, service, or interest that you have a lot of knowledge in or at least feel comfortable discussing, see whether that angle can work. Dr. Tom G. Stevens, PhD, says, “It is important to remember that self-confi dence is always relative to the task and situation. We have diff erent levels of confi dence in diff erent situations.” Th is statement is very important, because confi dence directly links to how others view you as a social engineer. Confi dence (as long as it is not overconfi dence) builds trust and rapport and makes people feel at ease. Finding a path to your target that off ers you the chance to talk about topics you are comfortable with, and that you can speak about with confi dence, is very important. In 1957 psychologist Leon Festinger came up with the theory of cognitive dissonance. Th is theory states that people have a tendency to seek consistency among their beliefs, opinions, and basically all their cognitions. When an inconsistency exists between attitudes and behaviors, something must change to eliminate the dissonance. Dr. Festinger states two factors aff ect the strength of the dissonance: » Th e number of dissonant beliefs Th e importance of each belief He then stated that three ways exist to eliminate dissonance (which should cause every social engineer’s ears to perk up): Reduce the importance of the dissonant beliefs Add more consonant beliefs that outweigh the dissonant ones. Change the dissonant beliefs so they are no longer inconsistent. How does a social engineer use this information? Approaching a pretext with lack of confi dence when your pretext says that you should be confi dent automatically creates dissonance. Th is dissonance raises all sorts of red fl ags and puts barriers up to rapport, trust, and forward motion. Th ese barriers aff ect the target’s behavior, who is then expected to balance out her feelings of dissonance, and kills any likelihood of your pretext working. One of the methods to counter that is to add more consonant beliefs so that they outweigh the dissonant ones. What would the target expect of your pretext? Knowing that will allow you to feed their minds and emotions with actions, words, and attitudes that will build the belief system and outweigh any beliefs that might bring in doubt. Of course, a skilled social engineer can also change the dissonant beliefs so they are no longer inconsistent. Although this is trickier, it is a powerful skill to have. It is possible that your appearance does not fi t what the target might envision for your pretext. You might think back to the show Doogie Howser, M.D. Doogie’s problem was that his “pretext” of being a top doctor never fi t since he was so young. Th at was a dissonant belief, but his knowledge and actions often brought that into the consonant beliefs of his “targets.” Just like the previous example, a social engineer can align his pretext with the target’s beliefs by their attitudes, actions, and especially their knowledge of the pretext. One example of this I recently saw in real life was at Defcon 18. I was part of the team that brought the Social Engineering CTF to Defcon. We saw many contestants who used the pretext of an internal employee. When presented with an objection like, “What is your employee badge number?” an unskilled social engineer would get nervous and either not have an answer or hang up, whereas a skilled social engineer would bring those dissonant beliefs into alignment for the target. Simply stating a badge number they found online or using another method they were able to convince the target that information was not needed, therefore aligning the target to their beliefs. Th ese points are very technical answers to a very simple problem, but you must understand that one can do only so much faking. Choose your path wisely. Learning to speak in a diff erent dialect cannot be glanced over quickly. Depending on where you live, learning to speak a diff erent dialect or with an accent can take some time. Putting on a southern drawl or an Asian accent can be very diffi cult, if not impossible. Once I was in a training class with an international sales organization and it had some statistics that said 70% of Americans prefer to listen to people with a British accent. I am not sure if that statistic is true or not, but I can say that I enjoy the accent myself. Now after that class, I heard quite a few people in the class practice their “cheerios” and “Alo Govenors,” which were horrible. I have a good friend from the UK, Jon, who gets very angry when he hears Americans trying to use lines from Mary Poppins in an imitation British accent. If he had heard this group, he might have blown a fuse. What that class taught me was that although the stats might say one accent is better than another for sales or just because you may be social engineering in the south or in Europe doesn’t mean you can easily put on the accent to make you appear local. When in doubt, throw it out. If you can’t make the dialect perfect, if you can’t be natural, and if you can’t be smooth, then just don’t try. Actors use vocal coaches and training sessions to learn to speak clearly in the accent they have to portray. Actor Christian Bale is from Wales, but determining that fact from listening to him is very diffi cult. He doesn’t sound British in most of his movies. Actress Gwyneth Paltrow took on a very convincing British accent for the movie Shakespeare in Love. Most actors have dialect coaches who will work with them to perfect the target accent. Because most social engineers cannot aff ord a dialect coach, there are many publications that can help you learn at least the basics of putting on an accent, such as Dialects for the Stage by Evangeline Machlin. Although this is an older book, it contains a lot of great tips: Find native examples of the accent you want to learn, to listen to. Books like Dialects for the Stage often come with audiotapes full of accents to listen to. Try speaking along with the recording you have, to practice sounding like that person. After you feel somewhat confi dent, record yourself speaking in that accent so you can listen to it later on and correct errors. Create a scenario and practice your new accent with a partner Apply your accent in public to see if people fi nd it believable. Th ere are innumerable dialects and accents, and I personally fi nd it helpful to write out phonetically some of the sentences I will speak. Th is enables me to practice reading them and get the ideas sunk into my brain to make my accent more natural. Th ese tips can help a social engineer master or at least become profi cient at using another dialect. Even if you cannot master another dialect, learning expressions that are used in the area in which you are working can make a diff erence. One idea is to spend some time listening to people in public talk to one another. A great place for this is a diner or a shopping mall, or any place you might fi nd groups of people sitting and chatting. Listen closely to phrases or key words. If you hear them used in a few conversations you might want to fi nd a way to incorporate these into your pretext to add believability. Again, this exercise takes research and practice.

**Using the Phone Should Not Reduce the Effort for the Social Engineer** In recent years, the Internet has come to dominate certain more “impersonal” aspects of social engineering, whereas in days past the phone was an integral part of social engineering. Because of this shift, many social engineers do not put the energy or eff ort into phone usage that can make it truly successful. Th is topic is here to show that the phone is still one of the most powerful tools of the social engineer and the eff ort put into using it should not be diminished due to the impersonal nature of the Internet. Sometimes when a social engineer plans a phone attack his thinking may diff er because using the Internet might appear easier. Note that you should plan to put the same level of eff ort, the same level and depth of research and information gathering, and most importantly the same level of practice into your phone-based social engineering attacks. I was once with a small group that was going to practice phone presentations. We outlined the proper methods, the tone, the speed, the pitches, and the words to use. We outlined a script (more on this in a minute) and then launched a session. Th e fi rst person made the call, got on the phone with someone, and messed up the fi rst few lines. Out of complete embarrassment and fear he just hung up on the person. Th ere is a very good lesson there—the person on the other end of the phone has no clue what you are going to say, so you can’t really “mess up.” Practice sessions can help you learn how to handle the “unknowns” caused by your accidentally altering something in your script that throws you off base. If you are not as fortunate to have a group to practice or hone these skills with, you will have to get creative. Try calling family or friends to see how far you can get manipulating them. Another way to practice is to record yourself as if you were on the phone and then play it back later to hear how you sound. I personally feel that using an outlined script is very important. Here is an illustration: suppose you had to call your phone company or another utility. Maybe they messed up a bill or you had another service problem and you are going to complain. After you explain yourself to the rep, telling her how upset and disappointed you are, and the rep does absolutely nothing for you, she says something like, “XY&Z is committed to excellent service; have I answered all your questions today?” If the drone behind the phone thought for one second about what she was asking she would realize how silly it is, right? Th is is what happens when you use a written-out script instead of an outline. An outline allows you “creative artistic freedom” to move around in the conversation and not be so worried about what must come next. Using the phone to solidify your pretext is one of the quickest methods inside your target’s door. Th e phone allows the social engineer to “spoof,” or fake, almost anything. Take into consideration this example: If I wanted to call you and pretend I was in a bustling offi ce to add to the pretext I was trying to use, I could simply grab the audio track from Th riving Offi ce (www.thrivingoffice.com/). Th is site off ers a track called “Busy” and another called “Very Busy.” From the creators: “Th is valuable CD, which is fi lled with the sounds people expect to hear from an established company, provides instant credibility. It’s simple, eff ective, and guaranteed!” Th at sentence alone is fi lled with social engineering goodness—fi lled with what people expect to hear from an established company. Already you can see that the CD is geared to fi ll expectations and provide credibility (at least, in the target’s mind, after his expectations are met), thereby automatically building trust. In addition, spoofi ng caller ID information is relatively simple. Services like SpoofCard (www.spoofcard.com) or using homegrown solutions, allows a social engineer to tell the target you are calling from a corporate headquarters, the White House, or the local bank. With these services you can spoof the number to be coming from anywhere in the world. Th e phone is a deadly tool for social engineers; developing the habits to practice using it and to treat it with utter respect will enhance any social engineer’s toolset for pretexting. Because the phone is such a deadly tool and has not lost its eff ectiveness, you should give it the time and eff ort it deserves in any social engineering gig.

**The Simpler the Pretext, the Better the Chance of Success** “Th e simpler, the better” principle just can’t be overstated. If the pretext has so many intricate details that forgetting one will cause a social engineering failure, it is probably going to fail. Keeping the story lines, facts, and details simple can help build credibility. Dr. Paul Ekman, a renowned psychologist and researcher in the fi eld of human deception, cowrote an article in 1993 entitled, “Lies Th at Fail.” In that article he says [t]here is not always time to prepare the line to be taken, to rehearse and memorize it. Even when there has been ample advance notice, and a false line has been carefully devised, the liar may not be clever enough to anticipate all the questions that may be asked, and to have thought through what his answers must be. Even cleverness may not be enough, for unseen changes in circumstances can betray an otherwise effective line. And, even when a liar is not forced by circumstances to change lines, some liars have trouble recalling the line they have previously committed themselves to, so that new questions cannot be consistently answered quickly.

Th is very salient point explains clearly why simple is better. Trying to remember a pretext can be almost impossible if it is so complex that your cover can be blown by a simple mistake. Th e pretext should be natural and smooth. It should be easy to remember, and if it feels natural to you, then recalling facts or lines used previously in the pretext will not be a task. To illustrate how important it is to remember the small details I want to share a story with you. Once upon a time I tried my hand at sales. I was placed with a sales manager to learn the ropes. I can recall my fi rst call with him. We drove up to the house, and before we left the car he looked at the info card and told me, “Remember, Becky Smith sent in a request card for supplemental insurance. We will present the XYZ policy. Watch and learn.” In the fi rst three minutes of the sales call he called her Beth and Betty. Each time he used the wrong name I saw her demeanor change and then she would say quietly, “Becky.” I feel we could have been giving away gold bullion and she would have said no. She was so turned off that he couldn’t get her name right that she was not interested in listening to anything. Th is scenario really drives home the point of keeping the simple facts straight. In addition to remembering the facts, it is equally important to keep the details small. A simple pretext allows for the story to grow and the target to use their imagination to fi ll the gaps. Do not try to make the pretext elaborate, and above all, remember the tiny details that will make the diff erence in how people view the pretext. On the other hand, here is an interesting tidbit: A popular tactic used by famous criminals and con men is to purposely make a few mistakes. Th e thought is that “no one is perfect,” and a few mistakes make people feel at home. Be cautious with what types of mistakes you decide to make if you employ this tactic because it does add complexity to your pretext, but it does make the conversation seem more natural. Use this tip sparingly, however you decide to proceed, keep it simple. Let me tie all this together with a few examples that I have used or seen used in audits. After some excellent elicitation on the phone, a nameless social engineer had been given the name of the waste removal company. A few simple Internet searches and he had a usable and printable logo. Th ere are dozens of local and online shops that will print shirts or hats with a logo on it. A few minutes of aligning things on a template and he ordered a shirt and ball cap with the logo of the waste company on it. A couple days later, wearing the logoladen clothing and carrying a clipboard, the social engineer approached the security booth of the target company. He said, “Hi, I’m Joe with ABC Waste. We got a call from your purchasing department asking to send someone over to check out a damaged dumpster in the back. Th e pickup is tomorrow and if the dumpster isn’t repairable I will have them bring out a new one. But I need to run back there and inspect it.” Without blinking, the security offi cer said, “OK, you will need this badge to get onsite. Just pull through here and drive around the back and you will see the dumpsters there.” Th e social engineer had a free pass to perform a very long and detailed dumpster dive but wanted to maximize his potential so went in for the kill with this line. While looking at his clipboard he said, “Th e note says it is not the food dumpsters but one of the ones where paper or tech trash goes. Which block are those in?” “Oh, just drive the same way I told you and they are in the third bay,” replied the security guard. “Th anks,” said Joe. A simple pretext, backed up by clothing and “tools” (like the clipboard), and the storylines were simple to remember and not complex. Th e simplicity and lack of detail actually made this pretext more believable, and it worked. Another very widely used pretext is that of the tech support guy. Th is one only requires a polo shirt, pair of khakis, and small computer tool bag. Many social engineers employ this tactic to get in the front door because the “tech guy” is usually given access to everything without supervision. Th e same rules apply: keeping the storyline simple will help make this particular pretext very real and believable.

**The Pretext Should Appear Spontaneous** Making the pretext appear spontaneous goes back to my point on using an outline versus using script. Outlines will always allow the social engineer more freedom and a script will make the social engineer sound too robotic. It also ties in to using items or stories that interest the social engineer personally. If every time someone asks you a question or makes a statement that requires you to think, and you go, “Ummmm” and start to think deeply, and you cannot come back with an intelligent answer, it will ruin your credibility. Of course many people think before they speak, so this is not about having the answer in one second, but about having an answer or a reason for not having the answer. For example, in one phone call I was asked for a piece of information I didn’t have. I simply said, “Let me get that.” I then leaned over and made it sound like I was yelling for a workmate: “Jill, can you please ask Bill to give me the order form for the XYZ account? Thanks.