Frauds, Spies, and Lies

and How to Defeat Them

by Fred Cohen, Ph.D.
With illustrations by David Cohen

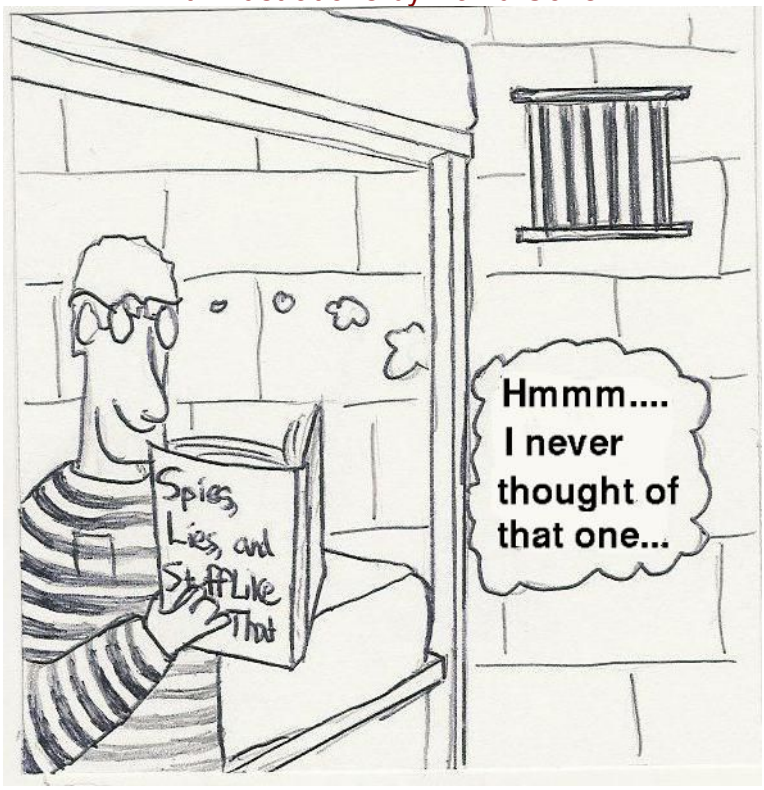


Table of Contents

Front matter

Frauds, Spies, and Lies
and How to Defeat Them
is

ISBN # 1-878109-36-7
Published by Fred Cohen & Associates out of Livermore, CA.

With illustrations by David Cohen

People who are successful at avoiding frauds read the fine print. As an example, this book is not really about frauds alone. It also covers issues in deception, intelligence and counterintelligence areas, some elements of magic, computer security, personal experiences, and all sorts of other stuff.

Well... in that sense it actually is about frauds. So I guess reading the even finer print is really important. So get out your magnifying glass and follow along with me. Once upon a time a loan officer at a bank handed me a mortgage contract. I started to read it - front to back - every word. Now I have some legal background having helped to automate a law practice, worked extensively on corporate legal issues for the various companies I have run, and worked on lots and lots of contracts. I also have some background in teaching computer-related law including teaching graduate classes with several Federal prosecutors. So at any rate, this contract says that I owe the finance fee regardless of whether I decide to pay it off early. It also says that this is true no matter who I talk to and no matter what they say. It says that when you sign the contract whatever was told to you does not matter at all - most contracts do. So eventually I decided to turn down the loan. What is my point? I have none. But I did get you to read all of this fine print with the deception that smaller was more important - but only to you. So now, using my skills at deception, I should tell you that you should tell others how important it is to read this part of the book and how they have missed the best part of it if they haven't done so. After all, you will not be able to get even in any other way. Something about the sins of the fathers should come to mind here. But back to my story. Yes - it continues for those who have stuck it out this far. This book really is about frauds and deception and intelligence and countering them, but it is also about what we have been seeing in the world around us in the United States. An ever deepening sense that perception is reality. But more on Larry King later... Enjoy the book.

I thought it would also be important to put in a disclaimer here. This book contains material that is not suitable for small children or people without humor or tolerance for other peoples' ideas. It includes a wide range of material that could be used for good or for evil, and of course I don't want to be liable for any of the evil things that it could be used for – including perpetrating frauds, choking people, using the book to trip folks, the kid leaving it on the steps, the pollution it creates when you burn it, or any side effects you may have in the afterlife from having laughed at certain things I may have said. All of these things as well as any other thing that happens as either a direct or indirect consequence of my having written this book is not my fault, and I take no responsibility and MAKE NO WARRANTY EITHER EXPRESSED OR IMPLIED ABOUT ANYTHING IN THIS BOOK. The law says I have to use large block letters to say that so you are amply warned.

But the law is not always all that useful in day-to-day life and, while it may come back to bite me, I really do not want to repudiate anything I have said here. So when you read the book, if you are offended by anything I have written, or if you feel your children or parents have been corrupted by it, remember, this warning was given to you and you could have looked at it before reading the book or buying it.

And furthermore, I am protected by the 5th amendment.. or was that the 1st? At any rate, you are free to say or NOT SAY anything you want, as long as it isn't yelling “Fire!” in a crowded theater when there is none (which I think the Supreme court failed to mention), and so am I. So get over it!

WARNING! READ THIS PAGE BEFORE BUYING THE BOOK!

That should do it I think...

1 Introduction

Frauds have been a subject of special interest to me for a long time because I encounter so many of them in my work in security. This book represents a collection of information about frauds, fraud types, examples, and stories of real frauds carried out over a period of many years. Once I started to describe the frauds, it was inevitable I would talk about spies and lies. So here we go.

Many folks ask me about writing books like this. I get questions ranging from "Is there a reference work on frauds and insider abuse?" to "Won't a book on frauds encourage people to commit them and help them do a better job of it?" With this book I hope to answer all of the questions. But of course that is an impossibility because there is no limit to human creativity. But there are limits to other things and, in addition to addressing the issue of frauds, which are acts of deception used for taking something from the target of that deception, I hope to address the issues underlying deception and its use in frauds and the larger question of how to counter deception and thereby counter frauds.

1.1 Overview

This book is organized as follows:

- **Frauds:** Things people do to take advantage of others through deception.
- **Deception:** The methods and mechanisms of deception.
- **Elicitation and intelligence operations:** How high-end deceptions are used by governments.
- **Counterintelligence:** What governments and others do about this to keep their nation-states safe.
- **Countering frauds:** This section talks about how frauds can be countered both by knowledge and by safeguards.

The casual reader might want to read only chapters 1, 2, and 6 on the first run through and come back for more later. More scholarly sorts, law enforcement, and government types might want to read the whole book. My graduate students had better read the whole book and everything on the Web site. The final is Tuesday.

1.2 What qualifies me to tell you about frauds?

I am not a policeman and I don't play one on television. So in this sense, I am not really qualified as well as a policeman with a lot of experience on the bunko squad would be at telling you about street frauds. But I do have a fair bit of experience in understanding computer-related frauds, insider abuses, business frauds, and other similar issues, because I have done a lot of consulting in my career, and in the security business, you encounter crime and criminals more than average folks do.

I have also studied some aspects of the issues underlying frauds in substantial depth. In particular, I know a great deal about deceptions because I have spent years of effort doing research and experiments involving deception and its use both for causing harm and for defending against threats that gather information in order to cause harm. I developed several computer software products and technologies that apply deception to counter attacks, did many scientific experiments that applied the results of other authors and researchers in the issues of deception to computer-related attack and defense techniques. Eventually I started teaching a graduate course on deception for the University of New Haven.

Once you start to study frauds and deceptions, it becomes a very interesting topic, but my experience also extends into the practical realm. No, I have never used deception to take things of substantial value from others. Rather, as part of my security-related work, I have participated in, led, and taught others how to participate in and lead "red team" activities. These are activities in which security specialists simulate malicious actors to identify, demonstrate, and help develop defenses against attacks. In my case, I have run a wide range of operations that involve the use of deceptions to gain trust of people, entry into facilities, access to information, and the capability to do a wide range of things that would be very harmful to the targets if I were not working for them. For those who used to watch the "Mission Impossible" television series, think of me as Mr. Phelps... but I don't work for the CIA. Just ask Valerie.

2 Frauds

Fraud is, in essence, theft by deception. Here are some examples of definitions that have been published in dictionaries:

- *Deliberate trickery intended to gain an advantage.* (Word Reference http://www.wordreference.com/definition/fraud)
- *In the simplest terms, fraud occurs when someone knowingly lies to obtain benefit or advantage or to cause some benefit that is due to be denied. If there is no lie, there may be abuse but it is not fraud.* (Workforce Safety and Insurance)
- *A deception deliberately practiced in order to secure unfair or unlawful gain.* (The Free Online Dictionary at http://www.thefreedictionary.com/fraud)
- *All multifarious means which human ingenuity can devise, and which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth. It includes all surprises, tricks, cunning or dissembling, and any unfair way which another is cheated.* (Black's Law Dictionary, 5th ed., by Henry Campbell Black, West Publishing Co., St. Paul, Minnesota, 1979.)

2.1 The two parts of a fraud

Yep, that's what it is. Taking by lying. Theft by deception. In other words, there are two parts to a fraud. *Lying* and *Taking*. I will sometimes use the word "*Deception*" instead of "*Lying*" and "*Theft*" instead of "*Taking*" because they are very nearly the same things.

2.1.1 Lying (Deception)

Frauds normally start with the lying part because without it the taking part taking is just theft, or if by force, robbery, or if from your house, car, or business, burglary.

People lie, and you and I are no exceptions. Perhaps the lies are usually trivial - so called white lies. They may even be ethical, like lying to a killer to keep them from finding their victim. Others are beneficial, like lying by exaggerating a bit to make someone feel

good about their appearance or manner of speaking when they feel insecure. Other almost automatic statements made in conversation may be untrue. Like when someone asks "How are you?" and you say "Fine, how are you?" in response without even thinking about it, despite having a little bit of back pain or maybe even a broken ankle.

So we all lie now and then, and in some sense we do it many times for an advantage of some sort. Lying to make someone feel good helps us gain their trust and befriend them. Saying you are fine when you are not is not always just a pleasant exchange. It projects health and well being. You might even say "Great!" when you are really only feeling fine in order to appear to be healthy and vigorous as part of a business meeting.

When does it become a fraud then?

2.1.2 Taking (Theft)

That's the second part of the equation. Lying in order to take something from someone else is fraud - theft by deception.

When one person tells another that they are beautiful and uses it to gain their trust, then gets them slightly drunk by taking them out on the town and going to bars, perhaps even takes them to dinner and a movie, then ends up trying to get into a physical relationship, they are potentially taking something (affection) by lying (telling them they are beautiful). But it is likely not a fraud, or at least not clearly one, because beauty is in the eyes of the beholder and what is taken was freely (in most cases) given. But if the liar starts discussing marriage and makes representations and promises, then there is the potential for a legal case on the charge of breach of promise. So there is a continuum here.

When someone takes something of value from someone else, whether it be money, jewels, time, business opportunities, etc. by using lies in order to trick the other person into giving those things without adequate or appropriate compensation, the lies and taking clearly become frauds.

2.2 Hundreds of examples of frauds

There are many examples of frauds, and you can probably find many of them in newspapers on a daily basis. If you use the Internet and look up "frauds" in your favorite search engine, you will find anything from intentionally staged car accidents to the "*Aztec UFO Hoax*" only a click or two away.

Frauds have been with the world for a very long time. There are examples of frauds described in the ancient "*Dead Sea Scrolls*" that form the basis for religious texts, and in almost every culture there have been frauds and laws to help the society and its citizens deal with those frauds. If I were to start trying to list every possible fraud it would quite literally take me forever to do it, and neither you nor I have the time to complete the task or read the result.

So instead, I will tell you stories of real frauds along the way. And of course what better time for such a tale than right now. After all, in a section with this title...

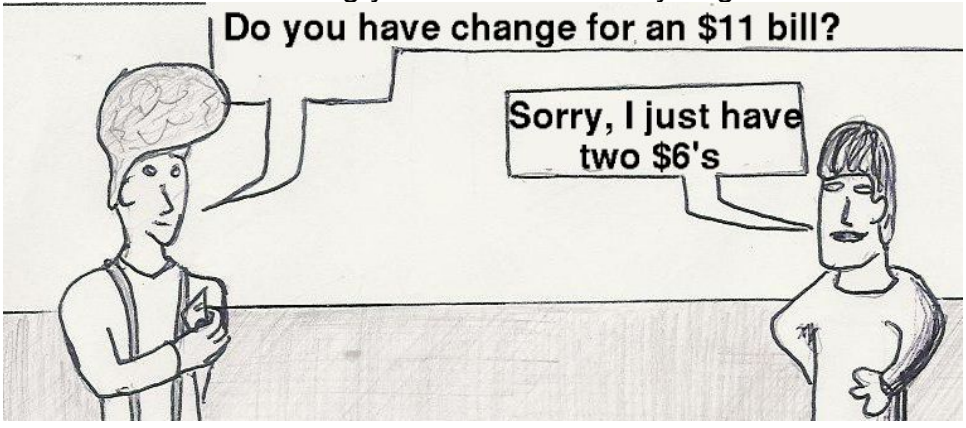
> *I once received an order for several hundred copies of a software product. This order represented substantial income to my company at the time. But the person placing the order, despite his good story, was not obviously trustworthy to me. So I processed the order, but I was not willing to grant credit to the individual and insisted on sending the goods Cash on Delivery (COD) as part of our contract. He agreed to it, but when the goods arrived, he refused to pay for them, so they were returned to me by the shipper for a small fee.*

Was this really a fraud? It sure seemed like one to me. He lied about wanting to get the order and being willing to pay for it COD. He later tried to get me to ship it on consignment but by this time I believed he was a fraudster. I sued him for breach of contract and won, but I never could collect because his business rapidly disappeared from its then present location. I lost some money on the exchange, and it certainly hurt me, but he never gained significant advantage from it.

Here is one more fraud I experienced a long time ago to help whet your appetite before getting into a more systematic discussion of frauds and more extensive lists of them.

> *When I graduated from college, I got a job in Texas and, while driving on the way to my new job from Pittsburgh, Pennsylvania where I lived, I encountered a small fair off the side of the road. I decided to go to take a break and have some fun. While walking through the fair that day I encountered a place where they were betting that I could not guess something or another about cards taken from a standard deck. I did a quick calculation of the odds in my head and determined that I should be able to win if I remembered correctly. So I took them up on it. After 3 tries at $20 a pop, I got the right answer and should have won $100. But then they changed the rules on me. So I demanded my $100 and they simply refused. I should have found a policeman and reported them, but being young and dumb, they offered the last $20 back and I took it deciding not to try to take them on (they looked bigger than me and there were many of them).*

Of course in this case the big mistake I made was in trying to gamble at such a place. Clearly when you play any game with a professional you need to be prepared to lose and when you play it in an uncontrolled setting you need to be ready to get defrauded.



2.3 50 ways to defraud a company

Actually, there are more than 50 here, but I use 50 because it gets people to look. And they are really not ways to defraud a company, they are just techniques people have used historically in financial frauds. But as you will read later, there are certain catch phrases and tricks that fraudsters use to entice you into their world. Welcome to mine.

These financial frauds includes selections from a list that was given to me by Ron Cole, who teaches about frauds to auditors all the time, examples from recent students of mine, some of whom work for big companies, and various ones I have come across in my wanderings and work.

2.3.1 Time shifts

Time shifts are a good place to start on discussing frauds. This is especially effective against computers and the institutions that use them for bookkeeping and auditing, because computers are so dumb that they don't understand time. As a result, they do all sorts of things that people would never do. Of course many of time shifts work without computers, but they would often be caught by humans.

2.3.1.1 Cookie jar reserves

Because companies often use an accrual instead of cash basis for accounting, it is often possible to write transactions as if they occurred in a year other than the one they actually occurred in. This shifting of money across fiscal years has many impacts, like reducing taxes paid in any given year (by spending before the end of year), or claiming higher earnings in a year than really occurred (by claiming income early and outlays late). The same can be done for a business run on a cash basis by holding income in cash until after the new year and paying bills sooner than they are due at the end of the year. The term "cookie jar" comes from people keeping spare money in their cookie jars at home. This is particularly effective in a cash business like a retail store or restaurant.

2.3.1.2 Revenue smoothing

In revenue smoothing, the perpetrator actively reshapes revenue to meet predefined goals. For example, if you get a large bonus for making a sales quota each quarter but a smaller added bonus for additional sales over that threshold, then it pays to not book the closed sales after the goal is met and use them for the next quarter instead. Similarly, you can book sales that have not yet actually closed but are about to close so as to make a quota that is close to the edge. A contract that has optional parts that add up to a lot of money but where the options are never exercised helps.

2.3.1.3 Premature revenue recognition

If it is a tough quarter, some executives might try taking revenues before they are realized. In accrual accounting, you are supposed to only recognize revenues from payments once the service required to fulfill those revenues is completed, properly anticipating future debt against those revenues. But if you count the income when payments arrive for services not yet rendered, like in the sale of magazines not yet delivered, the lie potentially turns into a fraud.

2.3.1.4 Deferral of expense

Deferring expenses makes for a more profitable year and this is sometimes used by executives rewarded for performance at the end of the year, especially when they are getting ready to leave the company. Many companies pay slowly and try to hold cash artificially long. For example, they may pay invoices only after 90 days or create artificial rules on payment processes so they can hold cash for longer periods. This translates into increased earnings on interest and better cash flow, but it is, in effect, stealing from those who they owe money to.

2.3.1.5 Manipulated fixed asset capitalization periods

Here we start to get a bit fancier. In this case, folks lie about the write-off periods for properties to allow expenses to be spread over a desired but inappropriate number of years. They may take a property that is amortized over 99 years and amortize a few extra years worth of it this year to make up for a shortfall, or they might not amortize it in a year when they don't need the deduction and then make up for it later.

2.3.1.6 Last year's money

Time is a funny thing in bookkeeping systems. Once the year is reconciled and closed out, it is largely ignored, but the database system that runs the computerized bookkeeping doesn't usually understand that, so... Take an account from the previous year that was not fully spent and use it to write a check to a vendor you have created for the purpose. The magic here is that the account has enough funds, so the transaction is no problem. If you keep it below management approval levels it doesn't require additional approvals. The books from this year's accounts are unchanged and nobody is likely to get any reports to reconcile expenditures because reports are usually run only from the current period. The overall books will still balance, so nothing should be noticed as out of the ordinary. You can do this until the account is empty, at which point you need to use a new account from a prior year. I use this one as an example that can be demonstrated on most systems. The details may be a bit more complicated, but you get the idea.

2.3.2 Cooked books

Sometimes people just cook the books. That's an old expression for just plain lying using the bookkeeping system to obfuscate it from anyone who doesn't want to look through all of the details.

2.3.2.1 Sell ownership may times over and fail

This one is from the musical then movie "*The Producers*" but it is such a classic that I just had to include it, and it does happen now and then. The producers of a Broadway musical sell percentages of ownership in the musical to old ladies, but they sell many times the total ownership, a few thousand percent. Of course if the musical flops, everyone figures they lost their investment, and the producers walk away with a profit. But as happened in the musical, it succeeded and the producers ended up in jail.

2.3.2.2 Fictitious revenue

Lying about the existence of revenues is a much more direct approach than the subtle cheating associated with things like shifting receivables, payables, and so forth. In this case, business owners simply claim revenue that never existed. Think Enron.

2.3.2.3 Reorganization or one-time charges

One of the ways I saw a large ($100 million dollar) theft covered up was in a one-time bookkeeping charge at the end of the quarter. Rather than admit to the theft, the financial institution decided that by rewriting the books they could claim the theft as a loss without revealing the details. Of course this was simply lying to the investors to keep them from running away from the bank, but such charges can also be taken in excess to create the illusion of success in the following periods or taken to cover up other crimes or misbehaviors. This is also sometimes called the "Big Bath".

2.3.2.4 Manipulation of performance numbers

In this fraud, the folks in control inflate sales or reduce costs to make performance numbers and get a bigger bonus. Of course a decent accounting process will catch this pretty quickly - within a year or two - but by then, other events can overtake the company and the cover up can be done with a small bribe here and there.

2.3.2.5 Financial statement manipulation

This is the simplest and perhaps most common and hard to believe of all. The executives simply lie on financial statements for their own benefit. If the accounting firm can't pick it up, or if they are part of the scheme, only the public gets bilked, and they only find out after the statute of limitations expires under new management.

2.3.3 False valuations

These include cases where management is supposed to determine a fair market value or some legally mandated value associated with some asset or so-called good will. When they lie about these the company may look better or worse. They also include methods used to manipulate the value of stock at opportune times, like to elevate when the executives are about to sell it or cause it to go down when they have a desire and the cash to buy a lot of stock. Insider trading and various schemes using the Internet are popular here.

2.3.3.1 Off book risks

In the days of the Sarbanes-Oxley Act, corporate officers are required to tell shareholders of substantial business risks as part of their annual statements in an attestation. The Chief Executive Officer or Chief Financial Officer can go to jail for misstatements because it misleads shareholders on the value of their shares and on the risks of holding them. Risks not recognized make the picture seem rosier. So it should be no surprise that executives at one company I reviewed got rather upset when they found out that they had a critical computer system that was necessary for the function of their business and that had no backup. This represented a very substantial risk of company collapse that their accounting firm had failed to recognize properly. This one was accidental, but the CEO was just as liable as if it were intentional. The lack of adequate redundancy in this case was because of a data center consolidation that had saved the company a few million dollars per year. The repair cost the company $10 million within a few months.

2.3.3.2 Over-valued accounts receivable

Many companies have uncollected receivable debts. But if these debts are also uncollectable, they are supposed to be written off instead of being kept as if they were going to be paid some day. When companies leverage this or other similar methods to act as if more is owed than really is owed, it is fraudulent in that it misleads the shareholders into a false sense of the value of the company.

2.3.3.3 Over-valued Inventory

When inventory does not exist or is not properly written off over time, it creates a misimpression of the value held by shareholders. Excessive inventory value leads to excess valuation and thus there are rules about how inventory is to be properly written off with time.

2.3.3.4 Misclassified investments

"Things are seldom what they seem. Skim milk masquerades as cream." (William S. Gilbert, English Lyricist, 1836-1911) expresses what happens when people manipulate the “fair value” of an investment. For example, when a penny stock is treated as the same value per investment dollar as a municipal bond, the shareholders are misled.

2.3.3.5 Misreported contingent liabilities

By changing the “fair value” associated with liabilities, a company can materially affect its bottom line. For example, I have seen companies claim that a cost reduction in processing yet to be processed outstanding contracts for work, reduced their contingent liabilities. Of course they were lying about the cost reduction by making assumptions about volumes that were not justified.

2.3.3.6 Manipulation of performance indicators

Manipulation can come in many forms. In one famous case, a California teenager who had invested in derivatives of a company's stock used an Internet forum to provide the illusion of near failure of the company. This drove the share price down, causing the derivative to increase in value, at which point the teenager sold the options, took the money, and eventually got caught.

2.3.3.7 Bid rigging

So called competitive bids are very often not competitive at all. For example, they create a seemingly endless list of requirements that happen to all be easily fulfilled by the bidder they want to have win. I have even been in bids that we won and the effort was then not rewarded, followed by a new solicitation for the same item where one of the competitors rebid just less than our original bid and won it. You can often tell a bid is rigged by the complex and inflexible specification and short lead times.

2.3.3.8 Bid rotation

When a small number of bidders know each other, they sometimes arrange to have lowest prices rotate among them so they all get high fees for their work but different ones win each time.

2.3.3.9 Pump and dump

This one involves manipulating stock prices by artificially creating demand through rumor, high pressure sales tactics, or multiple large orders. The price is "pumped" upwards and then when other investors join the trend, the original investors "dump" the stock in a rapid sell-off.

2.3.4 Goods manipulations

There are lots of ways to move physical things in and out of the company for periods of time in order to meet conveniences or for just plain thefts.

2.3.4.1 Channel stuffing

Introducing goods into supply channels can be used to make financial numbers when those goods are very likely to be returned. In the software business, major retailers buy on the condition of return if not sold within 6 months. As a result, anyone can sell a few million dollars worth of goods into the channel, but it won't get paid unless the products sell through. So it is really easy to create a business, get investors to put up a few hundred thousands dollars to manufacture, make a product of dubious value, get it into the market by pushing it into the channels on a contingency basis, and then claim great sales and receivables. This holds up for 6 months before it collapses, just enough time to sell the company for a lot more to someone else who doesn't understand the situation clearly.

2.3.4.2 Bill and hold

This is a favorite in the US Government. At the end of the fiscal year, money has to be spent or it returns to the taxpayers (an unacceptable option for most who work in the US government).So what folks do is take end-of-year money and buy things with it that don't really exist yet. For example, they will buy a million dollars worth of computers. But since they can't actually get the computers within the last 24 hours of the year when they order them, it is a fraud. But fear not - there is a way out. What they do is have an empty box shipped so that they can claim they have inventoried the arriving shipment. Then a few weeks or months later, they will figure out what they really want and the supplier will provide it to them. Of course should someone forget to actually get what they want, the money is still paid and the empty box treated as if it were inventory. It's best to do this with consumable supplies so that no inventory tracking is undertaken against the nonexistent goods.

2.3.4.3 Scrap or miscellaneous sales

The fraudster simply sells non-inventoried items, like scraps, for cash, and doesn't report the revenue.

2.3.4.4 Promotions manipulation

Did you ever wonder how it is that a particular person wins a drawing? This fraud has the perpetrator rig the winner of a promotion to a favorite vendor, customer, employee, or their family. Of course this is against the rules of most promotions, but it is commonly used in sales and marketing to create a better relationship with a key client. All you have to do is not announce the rules and award the prizes to the customer you most want to walk away happy. If done properly, this is even legal.

2.3.4.5 Resale or theft of company inventory

In this one the perpetrator sells company inventory for cash and the company records the goods as stolen for a loss. They may also commit insurance fraud along the way by trying to get an insurance company to pay for it, which is why insurance companies tend to investigate such things as possible frauds.

2.3.4.6 Theft of company resources/fixed assets

This is the most obvious one. The fraudster simply takes company supplies, goods, tools, etc. for personal use. Generally this works for anything that is not inventoried and for inventoried goods to the acceptable level of shrinkage for the company. If things start to exceed these levels, then they will be noticed, eventually investigated, and someone punished. In one case I heard about from a good friend, a large enterprise detected an individual taking small supplies from the company on a repeated basis. So they investigated and got a search warrant for the employee's farm. When they executed the search warrant they found an entire barn full of stolen goods amounting to more than $1 million in total value, taken over a period of many years, but never apparently resold or used for anything. There they sat in that barn.

2.3.4.7 Sell used computers to employees at discount

This one happened at a large enterprise. Old computers were being replaced and they were supposed to be disposed of, so the employee in charge of disposal had a bright idea. Instead of throwing them away and paying a disposal fee, he sold them off the back of a truck to other employees at a discount price. He then pocketed the cash and paid himself out of company funds as the

disposal company. I guess he figured his employer should have been happy that they paid what they expected for disposal while employees got discount computers and he made a profit. Somehow it didn't play that well to management.

2.3.4.8 Shorting

The vendor ships less than the quantity specified but bills for the entire amount. If the target doesn't do reconciliation, the vendor makes a bit more on every shipment. Targets often end up calling this part of shrinkage when they cannot trace it to a specific cause.

2.3.4.9 Insurance fires

Insurance fires are another name for arson that is used to recover insurance money for whatever was burned up, including things that may not have been there when the fire actually happened. As a rule insurance companies and fire departments investigate such things and arson is a serious crime, as is insurance fraud.

2.3.4.10 Advertising solicitation scheme

You are billed for advertising that looks like something you expect, but is not real. For example, a yellow pages bill that gets paid to Yellow Pages of Omaha when the normal fee is actually payable to a different company name. In many cases the subscriber may not even know that they are being billed twice a year instead of once.

2.3.5 Off book

These are things that don't quite make it to the bookkeeping system. Like large portions of the US Federal expenses that are "off-budget".

2.3.5.1 Barter

There is of course the rather large black market economy. This is often an all cash business, but there is also a large portion of it that is taken in-trade. This consists of non-cash and non-recorded exchanges of goods and services. For example, I can trade a hand-made table that you made for service on your computer. The government does not like this since they don't get to charge both of us taxes on the exchange. It is illegal but often tolerated. The so-called nanny problem that politicians have by paying a nanny in cash and never reporting the process to the tax folks is another

example. Today there are Web sites and bulletin boards that support this sort of trading and it forms a substantial part of the economy of many or most countries.

2.3.5.2 Forgotten bank account

Now it may seem strange to forget a bank account here and there, but it has been done. The perpetrators create a bank account that gets and sends money but that is not properly accounted for in the financial accounts of the company. Then all sorts of other things become easy to do. For example, take in payments and put them in the bank account, then write off the unpaid bills as uncollectable or forgive the debt in exchange for the next big order.

2.3.5.3 Bank account with similar company name

This is a favorite of folks like me who might create a company called International Bull Marketing and start intercepting checks sent to that other company with a similar name. Just make that check payable to "IBM". This is greatly aided when you put up a phony Web site - something like IBMdiscount.com is helpful.

2.3.5.4 Vendor kickbacks

This one is easy and completely outside of the bookkeeping of your company. You simply tell the vendor that they need to pay a “fee” to get the deal. It certainly happens all of the time, especially for deals in the former Soviet Union, France, Japan, China, India, ... In fact, just about everywhere you find some of it.

2.3.6 Banking and credit manipulations

There are various things that fraudsters can do with bank accounts. These are particularly popular among mid-level employees.

2.3.6.1 Coupon redemption

This one is popular among check-out staff. After customers are gone, they simply enter coupon information and take the coupon refund as cash. They know what is on sale and can readily get copies of the coupons from the newspaper or the store listing. This is sometimes done by the store owner for benefits as well.

2.3.6.2 Credit card number thefts

The number of different small-time credit card frauds is mind boggling. The one I will include here was undertaken by an employee of one of my companies in the 1980s. It is very similar to other frauds carried out all the time. The fraudster collects credit card information from customer purchases and then uses those cards to purchase something that is readily fenced or otherwise resold, like gold bracelets or wrist watches. They have the goods shipped to a relative's address or other similar location and pick the goods up when delivered. We caught the perpetrator after a week when a Visa customer reported the fraud appearing on their invoice. We then identified the perpetrator and provided full details to the credit card processor, but they did nothing because the cost of filing the complaint was not worth the effort to them. We fired the employee.

2.3.6.3 Cards to friends

If you work for a credit card company, which these days includes many companies that have their own credit cards or rebranded cards from other companies, it's pretty easy to approve friends for credit they don't deserve. In some cases thousands of "friends" have gotten credit cards with high limits and none of them were good credit risks. They spend and never pay off.

2.3.6.4 Redirected cards

Whether it is credit cards or banking cards or any other item in the mails with some apparent value, redirection can be used to take over the accounts. With insider assistance, the initial authentication can be forged and off you go to the credit limit. In one case an employee of a credit card company worked with a postal employee to move thousands of cards. The postal employee simply stuck labels on the outsides of the envelopes to redirect the mails.

2.3.6.5 Credit card slow burn

In some recent cases people from third world nations who have built up credit over periods of years charge their credit cards to the maximum amount allowed before leaving the country to return home. Perhaps this is their parting shot when they lose their permission to continue working in the country they are visiting.

2.3.6.6 Computerized card information thefts

Many cases hit the papers of thefts of large numbers of credit cards from computers or backup tapes. In these cases the information used by computers to verify cards is stolen. These fraudsters typically distribute the card numbers and related information to a few thousands perpetrators across the world for a fee per card number and these customers then start charging accounts.

2.3.6.7 Wire transfer

This is a simple one if you are authorized to or can convince the computer to send a large amount of money in a single transaction to a bank account somewhere that is unrecoverable. The biggest example I am aware of was actually a misdirected transfer of several hundred million dollars. The sender called the receiving bank which indicated that if they ever accidentally sent a similar amount back, the sender sender should feel free to keep it. The money was never returned. Because this sort of transfer is so potentially high valued, one of the things that I standardly do in protection assessments is look at electronic funds transfer (EFT) fraud potentials. In almost every company I have reviewed there is a potential for some level of fraud by a single individual. The largest amount I have been able to figure out how to steal in this manner was $1.2 billion. Yes - that's billion with a "B". I commonly find ways to take a few hundred million dollars using EFTs. Of course if you take this money in this way you had better be prepared to transfer it around a bit before extracting it as cash. They will try to track you down.

2.3.6.8 Phony company with similar name

I mentioned the notion of a phony bank account. The extension of this idea is a phony vendor with a similar name to a real vendor. An account is set up and funds are directed toward it. For example, Ivan’s Broadband Maintenance is set up as “IBM” and invoices from IBM are paid to it. A phony company is not quite the same as a phony bank account (described earlier) but it is very similar and banks today are harder to fool than they used to be.

2.3.6.9 Petty cash theft

Using the petty cash box an employee goes and gets donuts every morning for the office workers. They take money from the petty cash drawer, optionally filling out a form, but the money they pay is not the same amount as the cost of the pastries. They pocket the difference. Or in some cases they don't get the pastries at all.

2.3.6.10 Alter checks on their way to the printer

This takes advantage of the fact that in most computer networks, the actual checks go from the computer to the printer through a network. By attacking the network, the print file can be intercepted and altered, for example to increase your pay amount. This very thing was done by a British subject some years back and the extra money was used to pay for his University tuition. He kept track of the money and some years later, after the statute of limitations had expired, sent the company a check for the amount taken plus interest and a note describing how he had done it, so they could fix it for the future.

2.3.6.11 Cash back on credit card purchases

I like the credit cards that give cash back on purchases. What many folks do is make company purchases using those credit cards, then get reimbursed by the company for the purchases and get cash back from the credit card company as well. Of course this is the company's money that is being taken through a discount unrealized. The US government periodically asserts this relating to frequent flier miles by telling employees that they frequent flier miles are not theirs but the government's, but they then relent and the employees take the miles for vacations and so forth. You can think of it as a kickback or a bribe or whatever you like. Rebates can also be used this way.

2.3.7 Fake companies

The creation of fake companies is very useful in moving money in and out of real companies. The examples here are only the start of the different sorts of fake company frauds seen these days. The ease of creating a company using the Internet makes this all the more appealing.

2.3.7.1 Paper firm

A fictitious company is created to defraud another company. These days you can create a company for a few hundred dollars from over the Internet and build up a Web site for next to nothing to make it all look legitimate.

2.3.7.2 Phony vendors

Some folks have gone wholesale in this arena and created phony vendors, generated business for them, but never given a delivery despite having been paid for goods or services. This is the reason that separation of duties is mandatory according to accounting rules. It forces this to be the result of a collusion between at least two people in the target company.

2.3.7.3 Toner sales

Telephone solicitation frauds are fairly common. In this one the fraudsters sell poor quality printer toner to companies at high prices (for the quality provided) while still giving a lower price than the high quality producers.

2.3.7.4 Bankruptcy fraud

Given the record numbers of bankruptcies these days it should be no surprise that some have taken advantage of this legal approach. They borrow a lot of money and use bankruptcy to avoid debts - repeatedly - under different business names.

2.3.7.5 Big store

The big store is a place that appears to be a business but is, in reality, designed to bilk the target out of money. The store front proves that the fraudster is legitimate and running a substantial business.

2.3.7.6 Slow burn dummy supply company

To make real money in a longer-term fraud, some folks build up real business relationships with suppliers and customers. The key to this fraud is that the fraudster never invests much of their own cash. They start out by getting money from the target for a small order of goods that the target regularly buys in large volume, but sells it to the target at a lower than wholesale price. This costs the fraudster some money. The target then verifies that this is the real

goods, that the quality is high, and that it is, in every way, what they need and have been buying at a higher price. The fake supply company then builds up to higher and higher volumes, but only on pre-paid orders with increasing delays between payment and delivery as the volume increases. Before long they get the "big buy" order for hundreds of thousands of dollars, pre-paid, and walk away with the cash. This works particularly well because the target finds it hard to believe that the fraudster would walk away from their apparently profitable business that does such high volumes for a mere few hundred thousand dollars.

2.3.7.7 Reinsurance scam

Reinsurance is an industry in which insurance companies get insurance from other companies for enormous losses (typically in excess of $100M and sometimes far higher than that). Most of the insurance companies most people know about only pay off on claims from a few thousands of dollars of loss to a few tens of millions of loss. It is part of their risk management process to limit liability. Undercapitalized reinsurers sometimes pop up and lie about the assets behind them, or perhaps they write too much insurance for their available assets. They collect big premiums for reinsurance but have inadequate assets to pay out when they eventually get real claims.

2.3.8 Trading places

These frauds all involve swapping one thing for another, including various kinds of forgeries (trading a signature for none, a check for another, an amount with another, and so forth.

2.3.8.1 Skimming

Skimming is taking amounts from places where things are hard to notice or account for, such as returns or sales of scrap goods. Sales of scrap goods like iron are typically done by the ton. If there is a pile of scrap iron in the scrap yard and you load it onto a truck, there is rarely a detailed weighing to make sure of the weight sold. When you get to the buyer, the payment is often in cash. It's pretty easy to sell more or less, charge more or less, and pocket the difference - on both sides.

2.3.8.2 Slush funds

There are many companies with cash boxes or similar repositories where funds are put without receipts and then extracted as needed for unaccounted for purposes. It's often easy to take small sums from these places, but in some cases these can end up adding up to rather large sums. And since the accounting process is usually minimal to non-existent these funds can grow rather large if supported by those interacting with customers and suppliers.

2.3.8.3 Checks for cash

You sell goods for both cash and checks. But when you get a check in, instead of finishing off the sale, you take the check for payment, void the sale, and take cash in the same amount as the check from the register. Until the inventory reflects the difference, the fraud goes undetected, and if the amounts are within normal shrinkage amounts, it may go on and on.

2.3.8.4 Register thefts: under-rings

There are so many different forms of this it is beyond my ability to even count them. But in the general form, the person at the counter rings up less than is charged and pockets the difference. The problem comes when customers get their change and see what is rung on the register. Some fraudsters simply give less change than is due, while others turn the register display so that customers cannot see it. Some unplug the displays while others show a total that they then back out as the customer leaves.

2.3.8.5 Register thefts: over-rings

Over-rings are used to charge the customer more than the proper value for the items purchased. After they leave, the teller might even correct the transaction and take the excess cash.

2.3.8.6 Receipt alteration

For paper systems, it is often easier to create small errors. One example is the alteration of a receipt by entering a lower amount on the cash receipt than the cash received. The perpetrator then pockets the difference.

2.3.8.7 Invoice for goods never sold

Some people simply send invoices for common office supplies to companies and hope that the companies will pay them. It helps to know what kind of equipment they have, and this can often be gleaned by dumpster diving.

2.3.8.8 Underreported or unrecorded sales

For cash businesses, it is often easy to make sales and not report them. One approach is to take the cash and leave the loss of goods as shrinkage to be detected in inventory. This is doubly good for the merchant who writes the lost goods off of their taxes while collecting the retail value in cash. Of course if you get caught you can go to jail, and many have.

2.3.8.9 Unsecured cash or checks held overnight

The easy thing to do is to break in and steal the cash. Of course if you do this very often you will likely get caught. So an alternative is to take some of the cash along with some of the paperwork so that the overall till balances the next day. That's why many companies insist that there be an end-of-day reconciliation - but then you can always do it at lunch instead.

2.3.8.10 Altered payee

This sort of fraud consists of changing the name of the payee on a check and then cashing it. Another variation is telling them to make it payable to the Charleston and Alexandria Subliminal Healing (or they can simply abbreviate it to CASH).

2.3.8.11 Manual checks

In non-automated check systems, there is usually a way to write a manual check using the legitimate payee in the accounting records but putting another name on the check. Alternatively you might not record the check at all, but this is more likely to be noticed.

2.3.8.12 Resubmission of invoices

Resubmitting invoices against purchase orders that are not correctly marked as paid often ends up generating an additional payment. Of course with an insider involved this can become habit forming and catching these insiders is particularly important to success against frauds.

2.3.8.13 Over-billing customers

You can simply bill more than is owed and hope they never notice. Of course some will notice and then you need to compensate them for it, but not always. In one such scheme perpetrated against one of my employers when I worked indirectly for the government, a company had a monthly invoice arrangement for charging the company credit card for telecommunications services. These services were found inadequate to the need and canceled by the buyer - but the telecommunications company kept on charging the credit card. They were told to stop but simply ignored the notice. Then the credit card expired and they managed to find out the new expiration date and continued further. Eventually this went to the company legal council who determined that the cost of forcing the issue in a law suit was not worth the monthly loss that was being charged. I pointed out that fraud is fraud and it should be reported to federal law enforcement, but it apparently never was. The charges eventually stopped, but only after I spent a lot of time and effort pushing against the system. And the company kept the money collected even though they never provided the services.

2.3.8.14 Recovery of bad debts

While most bad debts don't ever get repaid in full, companies that write off a lot of debt may write off a debt then not report receipt of the money when it arrives. This off-book income turns into cash for those perpetrating the fraud. It is even possible to write off debt that you think will be paid and thus shift revenues over time.

2.3.8.15 Refunds

Many refund systems are far less well controlled than sales systems. As a result, refund frauds are fairly common. For cash refund systems, it is often easy to take cash and report it as a refund to a customer. Phony paperwork is easy enough to generate and, for the professional, even check-based refunds of goods not returned to inventory can be quite lucrative.

2.3.8.16 Transfer of receivable balances

The use of inter-account transfers provides a wide range of possibilities. One is to take cash from a payment, and then transfer the same amount from a long past-due account that will soon be

written off. The account about to be written off will be written off for that much more while the account that was paid looks consistent and the perpetrator walks away with the difference in write-offs as cash. Of course accounts that are going to be written off should not allow additional debts to be incurred, but systems are imperfect.

2.3.8.17 Redirection of double payments

Another similar fraud happens when someone overpays. The idea is to redirect the overpayment amounts on paper to old long-past-due accounts and then take the amount of the overpayment in cash. The long past-due account now has no more debt, the fresh account is paid in full, and unless the payer notices the overpayment, nobody will likely catch the exchange.

2.3.8.18 Redirection of bank loan funds

When companies get loans the money should be spent on the company, but sometimes folks decide to borrow money for a company purpose and spend it for personal purposes. If they are well positioned, the personal expenditure will go unnoticed and the debt will be added to the current debts without being questioned. After all, if the CFO says it is legitimate who will argue with them?

2.3.8.19 Write-offs

In another variation on the redirection of payments, the perpetrator steals money from a customer payment but keeps the customer happy by writing off the unpaid debt as uncollectable before the customer ever sees it.

2.3.8.20 Over-funding capital projects

While we may be used to governments underfunding projects then paying more and more forever against them, over-funding is another way to rip folks off. By over-estimating costs, budget is supplied for those projects. The perpetrator can then skim money or get kickbacks from contractors in exchange for the job and the job will remain within its budget as the individual extracts money.

2.3.8.21 Second check stock

In this one the perpetrator copies the check stock and uses the copies to write phony checks. This is particularly easy with digital copiers or scanners and printers that can rapidly make very good

color copies adequate for the human eye to be readily fooled. The nifty part of this fraud is how hard it is to get caught because you can cash the check almost anywhere. The countermeasure is systems that inform the bank of all details of all checks as they are written. The bank can then immediately spot a fraud and refuse payment. The perpetrator can often be caught with these defenses.

2.3.8.22 Forged checks

Of course you can use forgeries to sign checks inappropriately. This is fraud the old fashioned way. It is even easier with laser printers and scanners because copying the signature is really easy. If you want it to look like a real signature you can use a pen plotter to do the signature, leaving an indentation in the paper. In one case one of our assessment teams found a room full of check stock from a company ready to be printed on. Entry to the room was gained by using a credit card to open a door (slide the card into the lock and if the locking mechanism isn't a decent one you are in the room). With real check stock this is far easier.

2.3.8.23 Alter check amounts

A fairly common fraud technique sees the fraudster simply alter the amount on a printed check, for example, by adding a zero or two. While many individuals may notice it and not have that much money in their account, for large enterprises that process many thousands of checks per day, this goes unnoticed unless they use a system for sending check details to the bank for comparison.

2.3.8.24 Check bleaching

There are any number of methods for creating forged checks that look very real. One effective method uses bleach to remove the dollar amounts on checks. Once removed they are replaced with bigger figures and cashed.

2.3.8.25 Premium fraud

Employers sometimes steal from unemployment by lying about salaries or titles to lower premiums. This works because the premiums are based on representations by the employer and most unemployment funds are State run and don't check up on such things unless problems result on actual claims or someone files a complaint for some reason.

2.3.9 Shifting the load

These frauds shift money from account to account, or have the company pay for something they shouldn't, or have the company not get the benefits they deserve.

2.3.9.1 Eternal employee loans

This is often done by executives who have the authority to take advantage of the system and when there are poor controls in place. Of course these are the same executives that direct the audit processes so it makes it a lot easier to get away with. They simply loan money to themselves or their employees and never pay it back. Eventually the loans are written off as bad debts and the books even balance.

2.3.9.2 Loans to executives for a specific purpose

In this scam the company loans money to executives to purchase stock options they are entitled to, based on the collateral of the stock option they don't have till they get the loan. The loan is secured using something that does not have value yet which is, strictly speaking, not within the requirements of loans. This is commonly done because the options are owed and worth more than the amount loaned, but in some circumstances it is illegal.

2.3.9.3 Combining personal and company expenses

Submitting personal expenses such as telephone costs or electric bills as company expenses is fraudulent. But on the other hand, it is hard to tell the difference sometimes. For example, my small company includes an office in my house that uses a lot of power to run the computers and has company phones. While I can have separate phones for company use, the power comes from the house. So I should be able to legitimately write off part of the power bill for use in the business, but how do I tell that part of the bill from the part for the rest of the house?

2.3.9.4 Company credit cards

Many employees try to incur personal expenses on company credit cards so the costs get reimbursed as company expenses. In one extreme, a manager at a government facility decided to give bonuses to his employees beyond the bounds of the ones granted by the company. So he used his government credit card to charge

various things for the staff members and gave these things to the staff as gifts. It totaled something in the hundreds of thousands of dollars range, which was within his budget and amount that could be charged over time to his company credit card.

2.3.9.5 Personal expenditures

Executives have been known to bully employees into including personal expenses on company reimbursed expenses. This sort of bullying makes the separation of duties in most accounting systems unable to function properly and it compromises the integrity of the employee. Bullying of employees by executives is not as unusual as it may seem.

2.3.9.6 Phony expense reports

While people have always submitted phony expense reports, in the Internet age the whole process has become far easier to do. Because many of the "original" receipts are in fact emails or other computerized documents, it is usually trivial to print extra copies with altered dates. They are often quite literally indistinguishable from the originals. For sales staff, it is downright easy to create phony trips with client meetings and expensive meals.

2.3.9.7 Expense then refund

Return frauds are one of the most common and hardest for people to understand. They are all pretty simple in fact. You simply buy something that is expensed, submit the receipt and get the reimbursement, but return the goods for cash. Or you can do the same thing with a credit card unless it is a company card, in which case it will be reconcilable by the company if they bother to check.

2.3.9.8 Company services for personal use

Many people do this and it is often allowed to a reasonable extent by companies. An example is using the company telephone system or network for non-company use. While calling home to let the family know you will be late is usually allowed, calling the other side of the world for a few hours to run your independent business is out of the realm of the reasonable. In one case I worked on, employees were running a second company from within a venture funded company, including an entire information technology infrastructure and Web site with electronic commerce back-end.

2.3.10 Employee frauds

Not just employees who defraud the company, frauds involving false information about employees, false reports, non-existent employees, and so forth.

2.3.10.1 Ghost employees

No, I am not talking about friendly ghosts who actually work for you. These are fictitious employees who get paid but obviously produce no work. If you are really clever, you can even cut them from the budget for a bonus and excellent recommendation just before you leave the company. I encountered one such scheme on a fairly substantial scale during an investigation of a different matter. In this case the Vice President of Information Technology was outsourcing to his wife's company paying about 10 full time staff members who didn't actually do any work for the company. In fact, they were using the company's "green cards" to allow these people to gain illegal entry into the United States and then selling their time to a different company. Of course they were doing far more than that.

2.3.10.2 Employment of family members - nepotism

Many small company owners pay their family members to work in the business and this often includes family members who don’t really do significant work for the company. This reduces profits which takes money from the IRS, but it also pays them as employees so they end up paying taxes on wages as does the company. So in small companies it comes out about the same. But in bigger companies, it's a far different story. Executives may hire 4

children, a wife, an aunt, an uncle, and who knows who else. They may end up being paid tens to hundreds of thousands of dollars per year each, making for wages that could come to as much as a million dollars a year. And in many cases these phony employees do no work at all and don't even show up at the office. In some cases they even have other jobs. By doing this for a few years an executive can guarantee a pleasant retirement at the expense of the shareholders. And it works for many management level personnel who are not as high a level as you might think. Even shift supervisors can often get away with one or more family members on the payroll who do little to contribute to the bottom line of the company.

2.3.10.3 Unauthorized payroll advances

The algorithm on this one is pretty simple. Get a pay advance but never pay it back. Repeat… This typically requires some level of, at least passive cooperation by someone in payroll. Perhaps one of those family members you hired to work there might be willing to help out in this way?

2.3.10.4 Phony workers compensation claims

There are many billions of dollars per year in false workers compensation claims in the United States. These basically fake or exaggerate workman's compensation claims indicating that the worker can no longer work and thus should be paid for not working through the government funded mechanism. Soft tissue back and neck injuries are most common for these sorts of claims. There are even medical practices that specialize in this area and advertise to come and see them to substantiate your claim. Companies hate this because they have increased insurance costs when it happens. They sometimes hire private investigators to catch the frauds.

2.3.10.5 Phantom employee

The phantom employee is an employee who gets paid but doesn't actually exist. This can be used in many ways, but there is another version of this theme. In one case I am aware of, an employee for a public utility was getting a periodic review when it was found that their employment record was empty - not a single piece of paper

existed on them. They were called in for a meeting and asked about this, fell silent, left the building, and never returned. This is a clear indicator of a foreign intelligence operative. The subsequent research indicated that they never cashed a paycheck, and that the person they thought it was, was in fact working on the other side of the country in a different job and was not the same person.

2.3.11 Floats

Floats happen when there is a delay between an apparent financial action and the underlying transfer. Banks get interest on money between the time you submit a check and they make the cash available. This is called the float.

2.3.11.1 Lapping

Take money from a payment from company A. Then cover the difference with a payment from company B. Then cover the difference with a payment from company C. Continue indefinitely - perhaps even using some of the money to cover the original theft from company A.

2.3.11.2 Check kiting

Kiting is the use of the "float", or delay in processing checks before they are cleared to make it appear that you have more money in your account than you really have. By kiting around several bank accounts, you can make it appear that you have a great deal of money in each of several banks. In one of the first cases, the fraudster used a company mainframe computer to determine how long checks floated between banks and used this time lag to create recursive money movements with ever increasing values. He got caught when a computer failure for 2 days brought all of his accounts crashing to the ground. A common requirement that every employee take two weeks of contiguous vacation is sometimes used to cause such schemes to fail.

2.3.11.3 Credit Kiting

Credit kiting is far worse in many cases because when you use one credit card to pay off another, you gain increased credibility with both credit card companies and often can increase your credit limits. So you pay one card off with the other and have 30 days before the payment is due. At the end of the 30 days, you pay it off

with the one that is now available because it's last payment was made. No interest is accrued if payments are on time. You can pretty quickly build up a hundred thousands dollars or so of credit lines and then buy gold with all of the credit lines and skip out without paying.

2.4 The numbers game

I have used the false numbers 3, 7, and 50 for numbers in section headers for a reason. It turns out that in some cultures, the numbers 3 and 7 are regarded more highly than numbers like 139 or 14. Actually, 139 is pretty popular. So I used these numbers to "sex up the intelligence" on the book. Fifty is another story.

2.5 Person-to-person frauds

Many frauds are person-to-person. That is, they involve some sort of direct contact between one or more fraudsters and one or more targets. These come in a number of different forms and have common plots and themes. Chuck Whitlock has built a large part of his career on identifying and demonstrating scams. His book "*Scam School*", (MacMillan, 1997) includes detailed descriptions and examples. He has even perpetrated a broad range of these scams as part of his investigative reports, returning the ill gotten gains to the targets of his efforts. Many of those are included here along with some from Fay Faron (cited later) and some from my own experiences with others from here and there thrown in.

2.5.1 Fake paper and records

Fake paper is one of the most common techniques in frauds, simply because much of the world in the legal and transactional sense works on paper. Fake paper frauds generally involve creating some sort of falsification associated with pieces of paper.

2.5.1.1 Advanced fee scam

Any exchange where you need to pay a fee in order to get a prize, loan, or other thing of apparent value is likely a fraud. A good example of this is the lottery scam in which the target is told that they have won the lottery - in Scotland! For a fee we will transfer your winnings to you. They will, of course, provide adequate documentation (fake paper) to support their claims.

2.5.1.2 Autograph

In this fraud the target is fooled into signing a paper that is later used for a forgery. It may even be a multi-copy paper that has different terms on the back sheets than on the front. Most people don't read contracts before signing. I tend to read every word of them driving most sales people crazy. I have found loans for lower interest rates on my house that had penalties of the total interest if paid off in advance, and all sorts of other terms within these papers that ended up in no-sale conditions. Others have signed them only to find that they lost tens of thousands of dollars several years later when they went to sell their homes.

2.5.1.3 Automated debt scam

Early in the 1990s, the computing department of one of the banks issuing ATM cards had "gone rogue", cracking PINs and taking money from customers' accounts with abandon. A fraudster had figured out how to substitute personal identification number (PIN) information onto a banking card and use anybody's account with his own PIN. Today, of course, debit cards allow unlimited access to bank accounts without recourse, unlike credit cards that limit liability to customers.

2.5.1.4 Blind pool penny stock scam

In this fraud, the fraudster convinces the target to invest in a nearly worthless stock by artificially bolstering its value. The promoter keeps the price higher than the value and pockets much of the difference in a very high salary.

2.5.1.5 Coupon fraud

There are many versions of this scheme but basically, fake copies of coupons are made and pawned off as real to reduce the cost of goods. A variation on this theme is to sell books of forged coupons to others. You can often get from $20 to $100 for such a book of coupons.

2.5.1.6 Home diversion game

Two people visit the (usually old) target's house. One occupies the home owner while the other searches for cash and jewelry.

2.5.1.7 File segregation

This is the real way to get rid of your bad credit. The fraudster creates new identities for people with bad credit to allow them to get more money from credit companies. There are specific triggers for credit card companies offering credit to people, like entering college, etc. Since the processes associated with college course admission are not very hard to forge and the credit card companies rely on this data to offer credit, it is easy to get more credit than the cost of the courses you enter under a false name. You get the credit, use it, and go take your next course at the next school under the next name.

2.5.1.8 False credit improvement

When there's a real fraud there is also a fraudulent fraud. Lots of folks sell schemes to get rid of bad credit, but many of these are just frauds themselves. The person with bad credit pays cash and the fraudster never restores their credit at all.

2.5.1.9 Foreclosure forestallment scam

I am being foreclosed on this huge property and all I need is $50,000 to stall it till I sell the property. If you can just lend me the $50,000 I will give you a percentage of the sale price for helping me out. You will double your money in a few weeks and save me from losing it all. To make it more realistic, I can create fictitious documentation and even demonstrate my access to the home and property by using forged keys when the occupants are away. It is too embarrassing to ask one of my neighbors or close friends, that's why I came to you. After all, you are a man of integrity.

2.5.1.10 Foreign bank investment scam

Many Americans are unaware that investments in foreign banks can yield far higher returns than just interest rates. For example, Fred's bank in Manatutu brought in 25% return on investment in the first 6 months of its operation. Of course the problem is that it now takes a minimum of ten million dollars to be allowed to open a bank in Gualapantu, where we are currently trying to get the next bank started. I have personally put up half of that and I am looking for a select group of American investors who are willing to put of the rest of the money to start the first commercial bank in this newly

emerging tourist spot. You get the idea. I could go on for pages. These sorts of scams are particularly popular on the Internet where it costs almost nothing to send you an email.

2.5.1.11 Franchise fraud

Franchisers sells franchises for various purposes all the time. But some of them are fraudsters. In this case, they sell the franchise, perhaps even someone else's real franchise, but never fulfill, running away with the investment money. This can typically be done for $50,000 or more per target.

2.5.1.12 Front-end loading

This fraud puts a high cost for buying initial products with promise of discounts at higher volumes. Nothing is wrong with that of course, until you don't ever get the discounts. Front end loading is also a very legitimate tactic in business when a relationship is new and the risk of billing is compensated for by the higher rates. After a time, the rates are lowered in most long-term relationships.

2.5.1.13 Counterfeits

In any of these frauds, the perpetrator finds a way to trade fake money for the target's real money. The forgeries range from stunningly good to just plain color copier copies of bills. This was demonstrated in the movie "The Sting" as the initial con game.

2.5.1.14 Hot seat

The target is asked to deposit a lot of cash and leaves a deposit with the fraudster who palms the cash providing paper in its place.

2.5.1.15 Jamaican switch (419 frauds)

The target is asked to hold large sum of foreign cash for the “foreigner” who takes real cash as a deposit. These are also called 419 frauds because statute USC 419 covers these sorts of frauds.

2.5.1.16 Medical mills

Medical and legal professionals work with paid patients to defraud insurance companies through false claims. This is common in Medicare frauds to the tune of many billions of dollars per year. In many cases the people making the illegal claims get little of the money and are also themselves not what they appear to be.

2.5.1.17 Paper accident

A phony car accident is submitted to an insurance company for insurance payments. This is greatly aided by the use of a car of similar make and model from a local junk yard. It also involves changing vehicle identification numbers and so forth, unless someone from the insurer is participating in the fraud.

2.5.1.18 Pigeon drop

The target “finds” cash along with two fraudsters. One decides to ask a lawyer what to do. The phony lawyer puts the cash in “escrow” and holds “earnest” money while a full settlement amount is determined. The earnest money is from the target and obviously never returns.

2.5.1.19 Premium diversion fraud

In this fraud, the fraudster diverts premium payments from a real insurance company. As long as you don't actually have to file a claim, you may never know you aren't actually insured.

2.5.1.20 AAA con

The American Automobile Association (AAA) is certainly a legitimate organization, however, AAA member towers may not be as good as the AAA itself. In this scam, AAA member towers notice car problems with the target's car (or creates them) and offers to fix them for a fee.

2.5.1.21 Work-at-home scam

There are any number of promotions for work-at-home jobs where you can make money by stuffing envelopes, cruising the web, etc. There is generally an initial fee paid to the company to get the necessary equipment and background information, and of course the fee is never returned and no instructions are ever shipped. There are also legitimate companies in these sorts of businesses.

2.5.1.22 Work at home shipment redirection

This scheme uses work-at-home workers to redirect shipments so that fraudsters can launder their locations through others. For large scale thefts via credit card, for example, many orders are placed using the addresses of the work-at-home crowd and that group reships all of the goods for a small fee to the fraudster who is now

far harder to track down. The work-at-home people are dropped after a few weeks and the address of the fraudster changes so that by the time the credit card company finds the work-at-home locations they are no longer used and the work-at-home people had no idea they were acting for a fraudster.

2.5.2 Fake stuff

Just as people use fake paper, they also use fake things. Things that either don't exist or are not what they look like are used to get money from the target. Fake things are also a key ingredient in the "looks like it" examples, except in these cases they are predominantly window dressing rather than the object of the exchange.

2.5.2.1 Dirt-pile scams

The opportunity to invest in a fake, or even a real but played out, gold mine is compelling. It is even more interesting if it has long time frames for return on investment. The classic example is to assert that this mine was thought to be played out but demonstrate an analysis that says we can extract more value than the cost by a factor of five by using modern techniques. In fact this is often true and there are companies that do this for a living on a very large scale. But just because it is all true does not mean you are not being targeted by a fraudster. In fact, the other party may even believe what they are saying. Then we just call it a bad investment.

2.5.2.2 Gold brick frauds

This is a process that convinces the target that there is a gold brick from Germany in World War 2, silver coins from a recently discovered wreck, or some similar story. They sell you the phony merchandise somehow on the promise that you know its value better than they, or that they cannot get out of prison (in the evil foreign land that has Internet access of course), or that they have to care for their dying parent, so you are the ideal person to turn this gold brick into cash.

2.5.2.3 Treasure hunters

The gold brick fraud can also be extended into treasure hunts. There are of course legitimate sunken ships full of Spanish gold doubloons, and sponsors do get rich. But very few of them.

2.5.2.4 Running the buckets

This is a fairly common fraud used by painters and other similar service industry individuals who are generally poorly paid for their time and make up for it in materials. In this case, they charge for more paint than was used by making it look like a lot more paint cans were used than really were. All they need to do is bring in a bunch of previously used cans of paint and present receipts.

2.5.2.5 Loaded dice

The target uses regular dice while the fraudster uses loaded dice. The result is that the fraudster wins more and more often. Of course you can also load the dice against the target. If you are one of us, think about those “gimmel dreidels”.

2.5.2.6 Three-card Monte

There are a lot of people who are very skilled with card tricks and other similar "magic". Some of them use this skill for frauds. A good example is the game of three-card Monte. In this game, a shill (fake participant in the game) wins at the game. The target then loses again and again. The reason this is a fraud is that it uses slight of hand to "palm" (conceal) the card that the target is looking for. The shill comes in every once in a while to prove that you can win, and the target keeps losing, convinced that eventually they will win.

2.5.3 Looks like it

One of the techniques that my teams use a lot in full spectrum red teaming efforts for enterprises is based on looking like what you claim to be. We regularly walk into buildings (tailgate) behind employees, dress up like UPS drivers, act like we are leaving and remember something we forgot just outside doors, carry clipboards over where our badges should be, walk in as groups so that when one is challenged, the other can vouch for us, sit in a smoking break area waiting for folks on their break to come out so we can go in, and one of my favorites, get in an elevator that doesn't let you go to certain floors and wait till someone from one of those floors calls the elevator, then walk out. It looks perfectly legitimate.

2.5.3.1 Assumed identity scam

The fraudster assumes an identity and does what that identity would do to get something from you. For example, someone who looks like a parking lot attendant might take your key and drive away in your car, never to return. It is called assumed identity because the target assumes that the individual is what they look like. Chuck Whitlock demonstrated this in front of an Italian restaurant acting as if he were a valet parking attendant when in fact this was a fast food joint that would never reasonably be expected to have such a service.

2.5.3.2 Bank examiner scheme

In this process, someone properly attired claims to be a bank examiner outside a bank trying to catch a teller who is cheating in the bank. They get the target to take out money to prove that the fraud is underway and give the target a receipt for their cash which they claim will be used to convict the evil teller.

2.5.3.3 Cash drawer audit

In this maneuver, the fraudster walks in with a replacement cash drawer claiming to be an auditor and gets the clerks to hand them the drawers full of cash in exchange for the nearly empty ones so they can “audit them”. They walk out the door with the full cash drawers, never to return.

2.5.3.4 Computer repair

This is one of many methods used to gain access to computers. In this one a call from "computer repair" comes in to fulfill a work order having to do with a computer. This is used to gain entry and access to equipment. This works with surprising frequency. But in our security assessments we have a policy to never lie. So we tell people we are there on a security assessment and they let us in. It is true, of course, so we are not lying, but anyone else could have done the same thing as a lie and gotten in, so we remain ethical and moral while gaining the same effect. In most cases this works very well after getting past the outer perimeters and works better if you look like what you claim to be. Whitlock always got proper costumes and vehicles to perpetrate his sample scams with hidden cameras.

2.5.4 Much for little

One of the most common claims made by confidence artists is that they only take money from people who are greedy. Of course this is not true in most cases, but much for little is indeed all about this.

2.5.4.1 Bait-and-switch

This is a common and illegal practice in which sale items are sold out before targets get there, so they try to up-sell you something that you didn't originally come in to buy. You thought you were getting a lot for a little and it turned out you were getting little.

2.5.4.2 Hot goods for sale

In this fraud, the seller sells items very inexpensively on the street and claims that they are stolen to convince buyer. The boxes are "factory sealed" which proves that they are top quality and perhaps a sample is shown to entice the buyer to buy. Of course the sealed units are empty except for weights intended to make them seem legitimate. The target has to tell the police they were trying to buy stolen goods in order to report it as a crime.

2.5.4.3 Cash back on the deposit

In this process, the fraudster uses fake deposits to get cash back from a bank account. They take a real deposit slip into a bank and, using a fraudulent check, do a deposit to the real customer's account with a cash back of a few hundred dollars. The deposit convinces the bank teller that they are the legitimate customer while the cash back comes from that customer's account. The fake check never clears but it takes days before the bank finds out.

2.5.4.4 COD scam

In this fraud, a cash on delivery (COD) package is delivered unexpectedly. After collecting the fee, the empty package is left to be opened by the target. This usually means wearing the proper uniform for the delivery service.

2.5.4.5 Counterfeit product

The market in forged versions (knock-offs) of popular goods is enormous. One of the most popular knock-offs is Rolex watches because they are so expensive that you can sell it for a "great price" and make a lot on the deal. As an aside, most fake Rolex watches have a second hand that ticks while a real Rolex second hand has continuous movement.

2.5.4.6 Phone clone

Fraudsters sell long distance calls using stolen phone card numbers. They are very common in many large cities. In the newest versions, they collect cellular telephone information by electronic eavesdropping and then sell cell phones preprogrammed with the fraudulent numbers.

2.5.4.7 Tele-blackmail

Where there's a fraud, there's always a potential for another fraud. In this fraud, after defrauding a target, some fraudsters then try to blackmail the innocent employee under threat of exposing them to their boss for participating in the fraud.

2.5.4.8 Ponzi scheme

Ponzi was famous for taking money from investors promising to double their money in a few weeks. Essentially: "Give me $50 and I'll give you $100 in one month out of the resulting business I generate". He did it in ever increasing volume using new income to pay off old outlays and generating a lot of cash flow. He then walked away with the cash. He was caught of course. But miniature versions of this are quite common.

2.5.4.9 Chain letters and other pyramids

Most people have seen chain letters that say that you can make money by sending them money, adding a name to the list, and sending it to 20 friends. This is another version of the long-running pyramid schemes that get people to send the people who start them large sums of money. To make the letter more effective, fraudsters claim curses on those who fail to propagate the letter.

2.5.5 Love (or lost love) and relationships

Fraudsters take advantage of love, the loss of love, friendship, and relationships whenever they can, because it gives them extra leverage in gaining compliance.

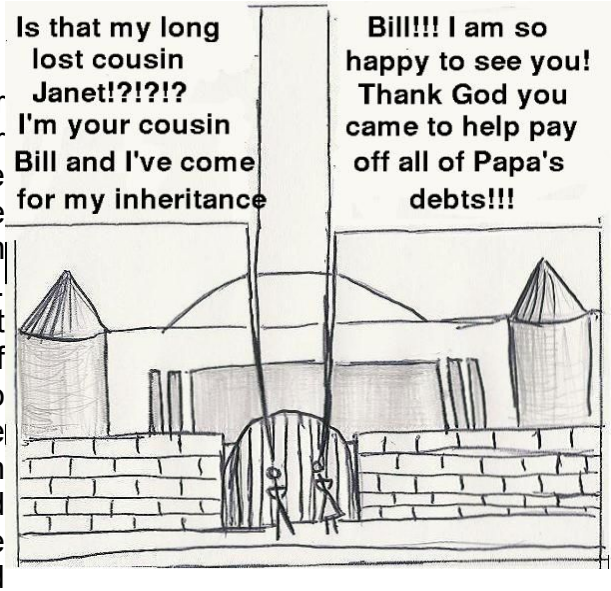
2.5.5.1 Friendship swindle

Lonely people are generally susceptible to many frauds because they long for companionship and fraudsters are willing to act like friends in order to take money from them. This fraud involves making friends with a relatively lonely person and starting to borrow increasingly large sums of money from them over time. It obviously never gets paid back. This is often done till the target has no money left at which point the friend disappears.

2.5.5.2 Obituary hoaxes

The fraudster in this case visits a bereaved person and demands repayment of non-existent debts from the deceased. This is greatly aided by forged documents or fake contracts that make it look legitimate. The family of the deceased is often stricken with grief and willing to do almost anything to be left alone by this fraudster.

2.5.5.3 Sweetheart scam



There are any number of cases where younger fraudsters get someone with money to fall in love with them and take them for all they are worth. They may even get married if necessary. Of course it is hard to differentiate legitimate love from frauds, which is part of why skilled fraudsters in this game rarely get prosecuted and often succeed at taking large sums from their targets.

2.5.5.4 Friends and family

The skilled fraudster can take advantage of friends and family of the target. They use the primary target as a reference or dupe to convince friends and family to support an effort that defrauds the larger group. This often involves things like appearing to want to help the primary target.

2.5.5.5 Mail order brides

Mail order brides are sold and resold. For a fee, this woman will come from Russia to marry you. Of course some mail order brides are legitimate, but do you really want to marry someone you have never met and who doesn't speak the same language as you from a completely different culture sight unseen? On the other side, some mail order brides are forced prostitution rings where women that offer themselves up as potential brides are kidnapped and turned into prostitutes.

2.5.5.6 Love shack

Young women entice men into bed and then claim to be underage. They extort money from the lover and eventually may report them to their spouses anyway.

2.5.5.7 Adoption frauds

Many people are so desperate for children that they decide to adopt one from the former Soviet Union or Africa or wherever. Many of these non-agencies are unregulated and use bait and switch tactics by offering something with false claims. Many don't even know what is being offered and are just wholesalers. And if you ever go to pick up the child you will find out what bribery is all about. They even tell you to bring cash and specify the amount - $15,000 US dollars perhaps, for their Russian “facilitator”. Be prepared to not get what you were looking for.

2.5.6 Injury and medical frauds

Injuries are really effective at bringing needed assistance, but fraudsters use fake injuries to extract money from owners of shops, insurance companies, governments, employers, and anyone else they can find.

2.5.6.1 Damage claims

Damage claims vary widely, but nothing works better for a quick hit of cash than a painful personal injury. The fraudster claims to be injured, threatens to sue, but takes a cash payoff instead.

2.5.6.2 Yank down

The term yank down stems from the nature of the fraud. In this fraud, the fraudster yanks down items from store shelves and feints injury as a result. They might then try to extort money from the store or individual to not report it.

2.5.6.3 You hit me with your car!

These specialists spend their careers getting hit by other peoples' cars and faking injury. They can step out between a van and a car and get a glancing blow that they exaggerate into a major injury.

2.5.6.4 My boyfriend will kill you

A favorite at bars for the young among us. A girl at a bar starts dancing with someone, acts very friendly, and when solicited for a closer relationship, the boyfriend shows up all upset and threatens to beat you up. Somewhere compensation becomes an option and you empty your pocket to avoid the fight.

2.6 Organization to person frauds

These frauds involve a person interacting with an organization, or what is meant to look like one.

2.6.1 Help me! and charity frauds

Help! I need somebody. Help! Not just Anybody! He-e-e-e-elp!!! Most people want to help other people in need, and this sort of fraud takes advantage of the desire of people to be helpful.

2.6.1.1 Need-help fraud

The target is told that the fraudster needs help and is convinced to provide money, use of a car, etc. as assistance. There are many different variations on this theme, usually involving at least one shill along with the fake victim, perhaps with a fake doctor, paramedic, or other person who plays the expert identifying the criticality of the need for rapid action.

2.6.1.2 Canister fraud

If you have seen children collecting for charities, you know that there is no way to detect a fake from a real charitable collection. In this fraud, canisters are used to collect for a fake charity. They are typically placed in stores and picked up when full.

2.6.1.3 Bail bond fraud

In this fraud, a midnight caller shows up to help a friend or neighbor of yours get out of jail. They pick up money at your door to help "throw their bail".

2.6.1.4 Katrina relief funds and more

A special place in Hell goes to the folks who start calling to get money illicitly when there is a natural disaster and people are dying. Whether it is hurricane relief, Tsunami relief, or Earthquake relief, whatever the life saving effort is, these people should be hunted down and stopped. You can expect that someone illicit will call you whenever there is a published outcry for help of victims. In 2005 these frauds were greatly facilitated by the large number of global natural disasters playing on the global news channels.

2.6.2 We can help you!

Any number of offers are out there to help you do one thing or another. Some are perfectly legitimate services while others are not. One of the ways you can tell the difference is how they go about their work. Generally, there is a script to these frauds that goes something like this:

- **Howdy:** A polite or interesting greeting comes first. "Hello Dr. Cohen, it sure is nice to reach you."
- **The compliment:** Next they compliment you. "You have been selected..." or "You are prequalified..." or whatever.
- **The setup:** Next they tell you what they can do to help you. "We can offer you free advertising..." or "We can help restore your credit".
- **The extraction:** Now they start asking questions. "We need to get your name, address, phone number (which they just called), email address, age, ... credit card number, take your order (or not).
- **Compliance tactics:** In case you back away, they come on strong to gain compliance. "You only stand to benefit from this offer." or "You won't get this chance again." or "Nobody else will give you credit on these terms."
- **The end:** When they have what they can get, they say goodbye politely and leave.

The compliance tactics are a dead give away. When I encounter these I am done providing information. They will try "It will only take a few minutes." or whatever, but don't buy it. Sales people often use time pressure, try to get you to spend time (sunk cost) so your investment with them causes you to not want to look elsewhere, and so forth. As a rule, if they try to get you to comply by changing their tone or implying force, walk away and count yourself lucky.

2.6.2.1 Credit repair scheme

There are any number of companies that will promise to clean up your credit ratings for a fee. In fact, for $500 I can get you a $250 line of credit at Fred's First Bank and I will report that you paid in full to all of the credit bureaus I subscribe to (which is none).

2.6.2.2 We can help you sell your products/services

I get phone calls every now and then from folks like "Who's Who" and other related groups that claim that it will help me to have my name listed in their database. They tell me it will increase sales to list me in the "Best researchers in the country" database or the "50,000 businesses about to explode" listing. And these are not bad public relations things to do, if you want to be listed all over the world as one of the top 500,000 egos in your specialty. But then this is also a great opportunity to gather information about you and then try to sell you something.

2.6.2.3 Phony job interviews (employer)

In places where jobs are hard to find, fake job listings are created to generate interviews where the interviewer collects information on the potential employee like name, social security number, date of birth, and so forth - all of the information required for identity theft.

2.6.2.4 Phony job interviews (employee)

Some folks who want to get information on a company will arrange to get a job interview by applying for a job with a fake resume. In the interview process they will ask questions and get tours of facilities that they can then exploit for the information on what is where, to plant a surveillance device, or to leave an explosive if sabotage or extortion is their goal.

2.6.2.5 Extracting information

In order to help you we need to get this information from you. Whether it's building a national directory or listing you in their sales portfolio, or what have you, lots of the scams claiming to help you are of course really helping themselves. They may collect and sell information on you, use your name and information to work a fraud remotely, perform the scam in order to start a relationship, or who knows what.

2.6.2.6 Need help selling your car? Why not give it away!

All you have to do is bring us whatever you have and sign it over and we will give you a receipt that you can use for a tax write-off. Yes, and people do give their cars and boats away for a theoretical tax write-off that may or may not convince the government.

2.6.3 The big con and related frauds

Fay Faron points out that most confidence efforts are specific “plays” and details the anatomy of a “con” ("*Rip-Off: a writer's guide to crimes of deception*", Writers Digest Books, 1998, Cinn, OH). But these standardized plays are only the beginning of the picture. Frauds have distinct elements to them based on human frailties. In this chapter I will try to review both what Fay says about some of the example scripts and some of the basic ingredients that make up the fraud schemes, why they work, and what they have in common.

2.6.3.1 The big con

The victim is sent to retrieve funds from a bank and these funds are taken by some method or another. This is a ten step fraud:

2.6.3.1.1 Find a target (the mark)

Victims are identified by particular characteristics, such as age, condition, appearance, etc. Old single people with little or no family are often targeted because of their high degree of susceptibility.

2.6.3.1.2 Gain target's confidence

This has to do with presentation, appeal, references, and similar things that gain confidence. Being a "disinterested stranger" seemingly caught up in a similar precarious situation might create mutual trust and confidence.

2.6.3.1.3 Show the target the money

Entice them with a win, or perhaps provide them a sample of affection or business success. Maybe it's a "golden opportunity", or perhaps just cash found on the street.

2.6.3.1.4 Tell the tale

The victim is told that they can make it big, get married to their dream partner, or get whatever they desire. Almost any story will do as long as it is credible to the victim. "I am an illegal alien and I can't be seen in the bank, so if you can just do this for me..."

2.6.3.1.5 Deliver a sample return on investment

The victim starts to get the things they wanted. "Hey Mary, that $25 you loaned me... I bet it on a sure thing and made $500. Here's $50 of it as appreciation for the loan. How would you like to be my partner in this?"

2.6.3.1.6 Calculate the benefits

The victim is shown how they can get so much more than they already have. "You know, if we did this again, we could make a bucket full of money."

2.6.3.1.7 Send the target for more money

They have to empty their bank account, provide everything they have, or what have you. "All I need is your cash to add to mine and we will be able to make a killing."

2.6.3.1.8 Take them for all they have

You need to get away with the desired returns. "Oh no! It didn't work this time. We have both lost everything we worked so hard for. You ruined me!"

2.6.3.1.9 Kiss off the target

Leave, perhaps in a manner so that the victim believes they got away with a good deal. "Here, you take the purse with the money, and we will meet tomorrow at the bank to finish the paperwork."

2.6.3.1.10 Keep the target quiet

Create a disincentive against reporting the incident. "Oh no! It's the cops. If they find me here with you, we will both be in a lot of trouble. You head out and I'll stall them."

2.6.3.1.11 Blow off

This is a general technique wherein the fraudster seeks to get the target to leave after they are taken advantage of by some deception. A common one is that the police are coming or perhaps that they want to leave in order to steal from the fraudster.

2.6.3.2 How a typical confidence operation works

Most confidence operations are done by small teams of people that work together. Team members have different sets of skills and experience, appearance, and roles in the little plays they undertake.

According to Faron, there are seven ingredients of a "con". She puts things in terms of the ingredient, a description, and the anatomical element. The anatomy of the confidence game involves each of the following elements.

1. The motivation (greed, love, loneliness).
   Free money for nothing.
2. The come-on (on opportunity to get what you want),
   Get rich quick.
3. The shill (a supposedly independent third party).
   In an area of expertise the victim doesn't know about, the independent expert (really a shill) makes the action seem legitimate. Everyone seems to agree on what to do.
4. The swap (take the victim's money while making them think they still have it).
   The target thinks they are holding the money.
5. The stress (time or other pressure).
   Some decision has to be made right away.
6. The block (a reason the victim will not report the crime).
   We will get away with it for some reason or another.

Generally, fraud teams of different sizes operate in different ways. This is discussed in detail later in the book, however a sampling will help whet your appetite for the long read ahead of you. The typical big con takes at least 3-5 people on the fraud team. A short con is usually 1-3 people. And most of the schemes described above take only one or two people. Compare this to the operations we undertake in testing security. We often use teams of 3-7 people to create more complex scenarios that are harder to understand and overcome.

2.7 The Internet: web of deception

The Internet is perhaps the richest breeding ground for deceptions ever created. A rumor can be started anonymously, forwarded in different guise to millions of readers, and believed and repeated by thousands, all in the space of a few hours. For deception, it is better than television ever was.

Generally, the more common and effective frauds that come from the Internet come in emails, postings to user or news groups, Web sites, spyware, and child exploitation.

2.7.1 Email frauds

Anyone who has never gotten spam has probably never sent or received electronic mail. Spam are those undesired messages you get in emails, and most spam is really also scam. The following are samples that arrived in one of my email boxes marked as spam between midnight and 10AM on a Saturday. I get about 500 per day in this particular email account and my spam filter kills off almost 99% of them, leaving me with five a day to manually delete.

2.7.1.1 Email scams I cannot read

Most of the spam emails I get are in English, but plenty are not. So if you get a message in Chinese and don't know Chinese, how can the scam possibly work? That's easy. The cost of sending out a spam email from a broken-into Web site (you can buy access through various organizations that break in and sell the service of sending out your spam) is on the order of a million spams for a few dollars. So if you splurge and spend $10 you can get a few million of these sent out. If one in a million answers and you can steal only $20 each it means you can make a few hundred dollars for every $10 you spend. So who cares if 90% of the participants can't read the messages. The 10% who can are still enough to make a good profit.

2.7.1.2 God: the scam

If you are a true believer, how can you resist helping God? No matter what God or gods you worship, there is a fraudster willing to leverage your beliefs for their gain over the Internet. Here is one for a Christian:

> Dear Fellow Believer,
> Greetings in the name of our lord Jesus Christ.
>
> To God be the Glory that I received Christ. Having known the truth, I had no choice than to do what is lawful and right in the sight of God for eternal life and in the sight of man for witness of God's mercy and glory upon my life.
>
> I have the pleasure to share my testimony with you; I am Mr. Paul Agbogwu, the Personal Lawyer of late Mr. Protasov Salenko, a Russian that lived in my Country Nigeria for 20 years before he died in the plane crash last year. He was a very good Christian, he is so dedicated to God but he was not married nor had any child till He died, may His soul rest in peace, Amen. Throughout His stay in my country, he acquired a lot of properties like lands, house properties, etc.
>
> As his legal adviser, before his death, Mr. Protasov Salenko, instructed me to write his WILL, because he had no child, he dedicated his wealth to God. According to the WILL, the properties have to be sold and the money be given out to a ministry or individual for the work of God. As his legal adviser, all the documents for the properties were in my care. He gave me the authority to sell the properties and give out the fund to a Ministry or individual for the work of God.
>
> In short, I sold all the properties after His death, as instructed by Mr. Protasov Salenko before he died. And as matter of fact, after I sold all his properties, I realized up to USD$6,000,000.00 (Six million US dollars). The total amount will be invested into God's work as instructed by the original owner. But Instead of giving the fund out for the work of God as instructed to me by the owner before his death, I converted the fund to myself with the intention of investing the fund abroad for my personal use. I was afraid of putting the fund in the Bank, because I have to give account to the bank on how I got the money. I

then packaged the fund in two Trunk Boxes and deposited the Trunk Boxes with a security company here in Nigeria. I did not want the management of the Security Company to know the content of the Trunk Boxes; therefore I registered the content of the Trunk Boxes as Family Treasures. Now the security company believes that what I deposited with them was Family Treasures.

I had a turnaround in my life few weeks ago, when I was watching a program on television. The name of the program is HOSSANA HOUR, and the man of God was preaching concerning Ananias and Saphira in Acts 5:1-11. After hearing the word of God, I gave my life to Christ and became a born again Christian. As a born again Christian, I started reading my bible and one day, the Lord opened my eyes to Ezekiel 33: 18 and 19 where the word of God says: "When the righteous truth from his righteousness, and committee iniquity, he shall even die thereby. But if the wicked turn from his wickedness, and do that which is lawful and right, he shall live thereby". From the scripture, I discovered that the only way I could have peace in my life is to do what is lawful and right by giving out the fund as instructed for the work of God by the owner before his death.

I have asked God for forgiveness and I know that God have forgiven me. But I have to do what is lawful and right in the sight of God by giving out the fund to the chosen ministry or individual, for the purpose of God's work as instructed by the owner before his death. After my fasting and prayers, I asked God to make his choice and direct me to a honest Christian or the chosen one that deserves this fund by his Grace. I then came across your address on the Internet as I was browsing through a marvelous site, and as a matter of fact, it is not only you that I picked on the site initially, but after my fervent prayer over it, then you were nominated to me through divine revelation from God, so these are how I received such a divine revelation from the Lord, and I then decided to contact you for the fund to be used wisely for things that will glorify the name of God.

I have notified the Security Company where I deposited the Trunk Boxes that contained the fund, that I am moving the Trunk Boxes abroad, and the security company has since been waiting for my authority for the Trunk Boxes to leave my country.

So if you know that you will use this fund honestly for God's work, then do contact me back immediately.

Waiting for your response.

Yours Sincerely,
Brother Paul Agbogwu.

It's nice to be trusted with administering millions of dollars for God and even nicer for stranger to help me do it. This is just the first step in this fraud. After you get in touch with them, they eventually get your banking information so they can electronically transfer the $6 million to you. They then use the information to empty your bank account. With brothers like that, who needs friends?

2.7.1.3 Help me get the money out!

This one, as all the ones I am providing here are unaltered by things like spelling corrections or other details:

Naturally, this letter will come to you as a surprise,since I am Senior Partner Mike Obi Jr contacting you to kindly assist me in the proposition below, which will be of mutual benefit to us both.

PROPOSITION

A salvadorean, Mr. Ramirez Videurre, 66 years of age and a very prosperous farmer made a huge bank deposit for investment in the sum of US$21.2 Million (Twenty one.two Million, United States Dollars) he named his wife Mrs. Helga Videurre as the NEXT OF KIN . I was called upon as an Accredited Attorney to the bank to sign and endorse documents to this deposit on Mr.Videurre?s behalf.

Unfortunately, Mr. & Mrs. Videurre were killed in the January 14, earthquake that rocked El Salvador ,killing thousands of people and 1200 others were declared missing. The bank management now mandates me (beirin the lawyer that signed and endorsed the deposit papers for the missing family to trace the family relatives of the deceased so that the fund will be released to them.

I was made to understand that they had no children.I made several efforts through the El Salvador High Commission in Lagos to contact any of the deceased family relatives, but to no avail.Failure to reach any of the family relatives of the deceased , the only option left for the Bank Management is to declare the deceased account dormant and revert the fund on trading and investment in the interest of the bank.

In order to avoid this development since it has so farbeen impossible to trace any of the deceased family relatives. I now seek your permission and assistance to have you stand as a distant relatives to the deceased. So that the fund can be released to you and we can use it for our mutual benefit.

I hope you do understand my concern in this matter, that if we do not use this opportunity to claim this fund , since the deceased relatives cannot be traced,the management of the bank will declare the deceased account dormant and revert the fund on Trading and Investment in the interest of the bank.For your assistance, you will be compensated adequately with(40%) of the total sum (55%) will be my own share while (5%) will be set aside to covering incidental expense made both at home and abroad prior to this transaction.If you are interested in assisting me with this matter, please send to me urgently via my the following details below:

*Full name, Company or Private Address
*Telephone and Fax number(s).

Upon receiving the above details from you, I willwork out every documents/proof representing you as the deceased BONA-FIDE distant relative and when this is done, you will be contacted by the bank for the release and collection of this fund, which willbe within one week of my receiving
the above details from you .

I will meet with you in your country for disbursement after the fund might have been released to you and also to discuss investment potentials as I will like to invest in your country with your assistance.Be assured that this transaction is 100% risk free,as I have taken care of all necessary modalities to enable a hitch free transaction.
Kindly ensure to treat this matter in strict privacy(Highly Confidential).
yours sincerely,

Mike Obi Jr.
SENIOR PARTNER

Wow! 100% risk free! Make millions for almost nothing! Does it sound familiar? I got several of these at different addresses. It's the same deal as the previous fraud. A multiple step process is used to get access to your accounts or credit card numbers or whatever, and they take your money.

2.7.1.4 I need your help!

Here's another variation on the "I need your help" theme.

> WILLIAM USMAN
> UNITED NATIONS REFUGEE CAMP
> ABIDJAN(COTE D'IVOIRE)
> CALL FOR HELP
> DEAR CHILD OF GOD
> PERMIT ME TO INFORM YOU ABOUT MY DESIRE TO GO INTO BUSINESS RELATIONSHIP WITH YOU. I AM WILLIAM USMAN THE ONLY CHILD OF MR AND MRS.MICHEAL USMAN, MY FATHER WAS A VERY RICH COCOA MERCHANT, BASED IN ABIDJAN, THE ECONOMIC CAPITAL OF IVORY COAST BEFORE HE WAS POISONED TO DEATH BY HIS BUSINESS ASSOCIATES ON ONE OF THEIR OUTINGS TO DISCUSS ON A BUSINESS DEAL. WHEN MY MOTHER DIED ON MAY 24,1996, MY FATHER TOOK ME SO SPECIAL SINCE I AM MOTHERLESS.
> BEFORE THE DEATH OF MY FATHER ON NOVEMBER 26,2003 IN A PRIVATE HOSPITAL WHERE HE WAS ADMITTED, HE CALLED ME SECRETLY TO HIS BED SIDE AND TOLD ME THAT HE KEPT A SUM OF US$10,500,000 (TEN MILLION FIVE HUNDRED THOUSAND UNITED STATES DOLLARS) IN A BANK IN ABIDJAN COTE D'IVOIRE. THAT HE USED MY NAME WILLIAM USMAN AS THE NEXT OF KIN IN DEPOSIT OF THE FUND HE ALSO EXPLAINED TO ME THAT IT WAS BECAUSE OF THIS MONEY HE WAS POISONED BY HIS BUSINESS PARTNER AND THAT I SHOULD SEEK FOR A FOREIGN PARTNER IN A COUNTRY OF MY CHOICE WHERE I WOULD TRANSFER THIS MONEY AND USE IT FOR AN INVESTMENT PURPOSE, SUCH AS:REAL ESTATE INVESTMENT OR STOCK MARKET INVESTMENT .
> SIR, I AM HONOURABLY SOLICITING YOUR KIND ASSISTANCE AS FOLLOWS.(1)TO PROVIDE A BANK ACCOUNT WHERE THIS MONEY WILL BE TRANSFERRED TO.(2) TO SERVE AS THE GUARDIAN OF THESE FUND,SINCE I AM A BOY OF 22 YEARS OLD.
> (3)TO MAKE ARRANGEMENT FOR ME IN YOUR COUNTRY TO CONTINUE MY EDUCATIONAL CAREER AND TO PROCURE ME A RESIDENTIAL PERMIT IN YOUR COUNTRY.I AM INCLINED TO OFFER YOU 15% OF THE TOTAL SUM AS A MODE OF COMPENSATION FOR YOUR EFFORTS AFTER THE TRANSFERING OF THESE FUND TO YOUR ACCOUNT IN YOUR COUNTRY.PLEASE, I WILL BE VERY HAPPY IF THIS TANSACTION WILL BE CONCLUDED WITHIN SEVEN(7)WORKING DAYS FROM NOW.
> I AM EXPECTING TO HEAR FROM YOU AS SOON AS POSSIBLE
> N.B:SIR,I WILL LIKE YOU TO GIVE ME YOUR DIRECT TELEPHONE AND FAX NUMBER IN YOUR REPLY OF THIS PROPOSAL.
> MAY ALMIGHTY GOD BLESS YOU AS YOU DO CARE FOR
> AN ORPHAN LIKE ME.ANTICIPATING TO HEAR FROM YOU.
>
> BEST REGARDS
> WILLIAM USMAN

You can guess what happens next... Your information, leads to your money becoming their money.

2.7.1.5 Gone phishing

The "phishing" scam is used by people who want to get access to your online banking information so they can empty your account. In this case, the trick is the universal resource locator (URL) that you are supposed to click on in the middle of the page to update your information. It looks like:

https://pcb.peoples.com/online/reset_profile.jsp

But in reality it is:

http://80.35.51.216/pcb.peoples.com/online/reset_profile.html

The difference is that the one displayed is the bank, while the other one is the fraudulent Web site. When you go there it has a form that asks for your user identity at the bank, your password, your social security number, your account number, credit card number, expiration date, and security code.

Dear Customer,

People's Online is designed using state-of-the-art technology to make it fast, simple, and reliable, so you can manage your finances without worrying about technical issues. If however, you are experiencing problems using People's Online on the Internet, we want to help you resolve the issue as quickly as possible.
A fundamental element of safeguarding your confidential information is to provide protection against unauthorized access or use of this information. We maintain physical, electronic and procedural safeguards that comply with federal guidelines to guard your nonpublic personal information against unauthorized access. Our mission is to reduce the instance of fraud.

Account Lock Out
Your account becomes locked out as a security precaution when your account has had more than 3 invalid passwords entered.
A User ID is allowed only three attempts before it is locked. Therefore we have locked your account until further assistance. To reset or unlock your checking account, follow the important steps from Unlock Service Page. By clicking the link provided below you will be sent to online secure service page:

https://pcb.peoples.com/online/reset_profile.jsp

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your confidential information. We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire Fulton Financial Corporation system.
About People's | Investor Relations | Press Room
© 2005 People's Bank. Member FDIC. Equal Housing Lender
Privacy | Terms & Conditions | Security Information

There are many of these created each day with results varying widely depending on the quality of the fraud and the gullibility of the target. They email them to millions of people each day so only a few have to be foolish enough to buy into it for them to win. They don't even care if you are a bank customer because the email is so inexpensive that they can simply send to every email address they can find. Some of them will be customers of the bank.

2.7.1.6 Blind date

This is a fairly recent variation on the oldest theme there is. For some reason people that get these tend to be people that visit adult sites on the Internet.

> Private message from: Michelle
> Message body: I am just so eager to know you XoXoXo
> Person's details: Platinum Blonde hair , Brown Eyes
> Age: 25
> To know this girl better & meet her, Log in now
> Takes one second!
> http://takingthugs.com/extra/gettingitgood-pg/
> No More Private Messages
> http://takingthugs.com/extra/gettingitgood-pg/getmeoff.php

The links lead to pornographic sites and date sites that you can join and pay for select services. You have to agree to something or another - but who reads the agreements anyway?

2.7.1.7 The lottery scam returns

It's an oldie but a goodie. The old lottery scam has worked for many years and it is still popular today.

> FAVOUR LOTTERY INTERNATIONAL BV
> ESCAMPLAAN 315
> 2105 KH
> DEN-HAAG,
> THE NETHERLANDS.
>
> ATTN:
>
> We are pleased to inform you of the announcement today 29th October 2005 of winners of the FAVOUR PROMOTION LOTTERY NETHERLANDS /INTERNATIONAL, PROGRAMS held on 15th of october 2005. Your email address attached to ticket number 21-134411314, drew the lucky numbers 11-10-20-13, batch number 6709/NL and consequently won the lottery in the 1st category. You have therefore been approved of a lump sum pay out of (€500,OOO:00) FIVE HUNDRED THOUSAND EURO ONLY in credited to file LOTTERY REF NO. SGIL/312128 This is from total prize money of EURO 30,000,000.00 shared among the seventeen international winners in categories B with serial number: RO/PR/11-C0225201.
>
> All participants were selected through a computer ballot system drawn form 15,000 company email addresses and 30,000,000 individual email addresses from

Australia,Africa, New Zealand, America, Europe, North America and Asia as part of International Promotions Program, which is conducted annually.

CONGRATULATIONS!!!

Your fund is now in custody of a Security company insured in your FILE REFERENCE. Due to the mix up of some numbers and names, we ask that you keep this award strictly from public notice until your Claim has been processed and your money remitted to your account.This is part of our security protocol to avoid double claiming or unscrupulous acts by participants of this program. This lottery program was promoted by our group of philanthropist headed by the Netherlands Government. We hope with a part of you prize, you Will participate in our end of year high stakes (€5,000,000.00) Five Million Euro, International Lottery. To begin your claim, please contact your file/claim Officer:

MR. BARRY HOOK
FOREIGN SERVICE MANAGER
DEN HAAG,
THE NETHERLANDS
TEL:+31-612-283-855
EMAIL:favourlottery@netscape.net

Please be informed that NON RESIDENCE of THE NETHERLANDS will be required to make a NON DEDUCTABLE advance payment of processment and legal documentation charges of (€998 .10 Cent) Nine Hundred And Ninety Eight Euro Ten Cent, to enable our legal department acquire Notorisation papers from the Court prior to award payment policy as required by the paying Securiry Company. Please be aware that your Paying Authority will Effect Payment Swiftly upon satisfactory Report, Verifications and validation provided by our Processing Agent; that would be designated to your file. For due processment and remittance of your winning prize to your designated account of your choice.

Remember, all prize money must be claimed not later than 5th of November 2005. After this date, all funds will be returned as unclaimed. NOTE: In order to avoid unnecessary delays and complications, please remember to quote your reference.And batch numbers in every one of your correspondences with your agent. Furthermore, should there be any change of your address, do inform your claims agent as soon as possible. Congratulations once again from our team of staff and thank you for being part of our promotional program. Note: Anybody under the age of 18 is AUTOMATICALY DISQUALIFIED. And batch numbers in every one of your correspondences with your agent. Furthermore, should there be any change of your address, do inform your claims agent as soon as possible. Congratulations once again from our team of staff and thank you for being part of our promotional program. Note: Anybody under the age of 18 is AUTOMATICALYDISQUALIFIED.

Yours sincerely,

Mrs.Rita Van De Muller
(Lottery Coordinator)

All I have to do to collect my winnings is send them money or information that they can use to steal money from me. In this case, as a non-resident, I have to send them a fee. Just push the [delete] key.

2.7.1.8 Cheap drugs and misdirection

The United States has a drug problem. No, not that one. The other one. The problem is that drugs are expensive here. Artificially expensive compared to the rest of the world. And the drug lobby manages to keep it that way with the help of the politicians. As a result, there are more frauds and scams related to buying drugs for less on the Internet than flies in all the barns in Kentucky (Hi Tom!). This is a drugs for sale over the Internet example:

> Effectively, it is identical to Pfzier viagra but much less in price.
>
> Chemically, GSC-100 is identical to the brand-name version and works just as effectively.
>
> You will not be disappointed. Delivery is Guaranteed.
>
> Sincerely,
> Carmella Falkowski
> Visit the customer-friendly site

The link leads you through a series of sites that extract the user name for further spam and then you go to:

http://www.affordablegenericdrugs.com/

This site looks quite legitimate, and they sell all of the brand name drugs as well as lower cost chemical alternatives. Legitimate, except of course for the fact that someone spams people and collects personal health related data on them before leading to the, possibly legitimate site.

2.7.1.9 Lose weight fast

It is estimated that most people in the US want to lose weight.

> We receieved your request for information on natural suppressants to help l0se weight.Our company Nutritionist's; Susan Miers & Mary-Anne McWhirter have found a solution for your weight problem.
> Solution:
> Susan & Mary-Anne reccommend a 2-4 month supply of MS-HOODIA!. Most of our clients have L0ST anywhere from 10-30 Ibs within 2-3 weeks.
> Recommended Supplier:
> http://supergreenhoodia.com
> *This recommendation is not available in retail stores until February 28th, 2006. This is one website that carries the product.
>
> (R)-emoval (S)-ystem on our Site- 2005

The misspellings are common in low quality frauds and spam. You go there, give them a lot of personal data, and they exploit you.

2.7.1.10 Home a loan

Want a home loan? Up to $401,500 or more? here you go. And you are pre-approved! I guess this means that you are trustworthy and that they have looked it up. It is interesting they they give a specific number like this and as you will read later, this makes it seem like they know some specific reason that you would specifically need this amount or that they have determined that this is the amount of credit that you personally can get. Of course they do not have any details at all, but it looks more specific to you this way.

> Dear Home-owner,
> You have been pre-approved for a $401,500 Home Loan at a 3.25% Fixed Rate.
> This offer is being extended to you unconditionally and your credit is in no way a factor.
>
> To take Advantage of this Limited Time opportunity all we ask is that you visit our Website and complete the 1 minute post Approval Form.
> Enter Here
> Sincerely,
> Julia Abernathy
> Regional Manager

The form looks legitimate enough but the information gathered is a bit invasive. It is likely that if you pursue it further you will provide enough information for credit card fraud and identity theft.

2.7.1.11 Rolex on sale!!!

Some Internet sales are legitimate while others are not. Buying a Rolex watch worth $1000 for about $250 is clearly a fraud, but many people buy fake watches and jewelry and never know the difference. The BEST prices and JUST FOR YOU! Nobody else could have gotten this offer. I got it on each of 5 accounts in an hour. If you only have one email account this looks personalized, but this one clearly is not. Look out for anything that seems personalized but that is not from someone you personally know. They are trying to build trust to take advantage of you.

2.7.1.12 Remove me!

Don't you bet on it. Many if not most of the "remove me" links and mechanisms on email frauds and scams are used primarily to gather more information on the target.

- If you click to get removed you are going to have to tell them your email address at least, and this will cause them to be able to verify that a live human being is at the other side, making your address all the more valuable because it is now verified.
- If your emailer looks up graphics from online sites in order to show you the email, the links used to do this typically have enough information to also confirm that your email address got the mailing, again confirming your presence, and perhaps even telling them more about you based on the information provided by your mailer or Web browser.
- If the email has a Trojan horse embedded in it and you read it the way it is intended to be read, your computer will have spyware planted within it to give them access to your computer, including things you type in - like credit card numbers and so forth.
- Many removal sites will tell you that all of this is untrue. While some are legitimate and may actually remove you, most are simply confirming your address - even if they say they are not.

Here is an example:

> IMPORTANT MESSAGE…
> Facts:
> Some people think that by removing themselves from some companies email list, they are confirming that there email address is valid. This is NOT TRUE in most cases. If you're reading this message then your email has already been confirmed.
> In accordance with recognized or accepted standards or principles, most marketers including US, have no interest in sending offers to people that have no interest in making any online purchases. It just doesn't make good business sense and wastes your time and our resources.
> When you unsubscribe from us… you will not receive another email from us (Period). This goes for all future products and services. We just ask that you give us a few days to remove your email.
> WE DO NOT SELL OR TRADE OUR DATA WITH ANY THIRD PARTIES, EVER!

How can you stay safe from all of this? Just delete it before you even look at it. I should note that this particular removal actually worked! A real rarity. Of course they also probably sold the address to others, but I didn't get more of those particular spams.

2.7.2 News group and chat room frauds

News groups and chat rooms are common ways to spread information on the Internet. While the vast majority of newsgroups are themselves legitimate, they are abused by advertisers and marketers and exploited for advantage by fraudsters under the guise of multiple personae. Or is it just good marketing? Chat rooms are smaller venues with more direct and real-time interactions. They tend to be used for more short-term frauds and to generate physical actions on the part of the target.

2.7.2.1 Fictitious people and personae (covert marketing)

In newsgroups, one of the most effective tactics is to create a set of people who support a desired position. This brings an enormous advantage over other individuals who join the group for meaningful interaction.

The process is rather straight forward. The fraudster creates several identities on the Internet and creates personality profiles for each of them. Within the forums of interest, they sign up groups of these personae and inject them into the forums with various views on information of interest. The net result is a magnified effect on the group.

A good example is in the sale of technical mechanisms, for example widgets and sprockets. There has been an age old debate over which is better - the widget or the sprocket, and of course it depends on the specific application. But in areas where they are in head-to-head competition, mailing lists debate the issue. If there are five vocal individuals in the group with three of them in favor of sprockets, by adding two more in favor of using widgets and giving them complimentary points of view, the weight can be rebalanced.

But getting even more clever, the fraudster can add a sprocket fan that is abusive, sends excessive postings, spells badly, and swears a lot. If they give really bad reasons that they like sprockets and explain how well they are doing by pointing out really bad results that they claim are the result of their brilliance in applying sprockets, people will run to the widgets.

2.7.2.2 The group approach to fraud

While an individual in a group using the magnifying effects of multiple personae can succeed, an even more effective approach is the use of real groups and application of the results on group psychology to the fraud.

Using their understanding of group dynamics, a skilled fraudster can do even better. And don't mistake fraudsters for idiots or fools. In California jails, many of the gang members take correspondence courses in psychology and marketing, and they use the material to create more effective frauds and to build up their criminal skills.

2.7.2.3 A class-ic example

In one of my graduate classes in deception, my class did a project with the goal of manipulating opinions in a group on the Internet. The experiment was about generating interest and beliefs supporting an article I had previously written about Chinese information warfare against the US indicating that the Chinese had won. They have, by the way, so we were only supporting the truth. Or at least the article that asked the question was an honest attempt at exploring the issue.

In this project, the class members looked up the members of the list, did background research on them, and created a plan for each of a set of people that were group leaders. The plan was to get the leaders to look into and buy into the notions underlying the paper. The goal was to build group consensus by swaying the leaders and having them sway the rest of the group. Without going into all of the details, it worked very well. Within about 4 weeks, the key group opinion leaders were stating that they agreed with the contents of the paper publicly.

2.7.2.4 Spam the list

Of course you don't have to act like you are a part of the group to join a group and abuse the privilege. Unmoderated mailing lists can be joined, in some cases automatically with computer programs, and then used to spam the group with whatever advertisement or other junk the fraudster wishes to send.

List spammers are rapidly dropped from lists, after only a few postings typically, but if a list has 1000 people interested in a specific area that the fraudster wants to go after, they get several messages to 1000 people in a few minutes after spending a few minutes signing up. And even manual signups to lists are not very expensive if they are outsourced to China or India. If it takes one minute of effort per signup, and labor costs $8 a day (expensive) that means that they can sign up to 480 mailing lists per day and spam 480,000 people each day for a cost of $8 or so. And of course they can do it every day. All they have to do is get one person in a million to send $100 to get a return on investment that most businesses would love to get.

2.7.2.5 Chat rooms

Chat rooms are used today for person-to-person frauds that don't require physical presence and for emotion-related frauds. The typical scenarios build up an Internet relationship by real-time interaction where the fraudster emulates what they think the person on the other side of the chat wants to see in them. If it is a fraud designed to entice an Israeli teenager into a Palestinian ambush (which did happen a few years back), they will act like a Jewish girl who just wants to meet a nice boy. If it is a person who wants to steal things from your home, they will act like a friend and find out when nobody will be there. And then there is the child exploitation abuse of chat rooms.

2.7.2.6 Child solicitation and worse

Lists directed at children are abused by a different sort of fraudster. These sick individuals claim to be children in order to get into conversations with children. They then leverage these interactions to gain information on the child which they exploit for crimes against those children. Chat rooms are very popular with child molesters. They meet children, play like they are also children, start to introduce sexual subjects, get the children talking, and arrange a meeting. The meetings almost always involve sex with the minor and the fraudsters who do this are almost all middle-aged men. More on this later.

2.7.3 Web site frauds

Web sites are used for advertising, for providing information, and for a widening range of application interfaces. Just as email pushes active content out, Web sites passively provide similar content to readership on a pull basis.

2.7.3.1 Information gathering from Web sites

Web sites are often used to gather information on those who visit them in order to turn the information into profits, and they are often used in conjunction with other communications elements in perpetrating frauds. One approach is to sell something legitimate at or below cost to gain personal and credit card information required to steal goods using the target's credit card.

2.7.3.2 Fraudulent offers for sale

Lots of sites are used to offer low low prices on goods that are never delivered. Others do a bait and switch, sending you something very different from what you thought you were getting. Some have similar spelling and appearance to name brands but are not the same. This is far more common in the Internet than in physical stores where you get to look and see the goods you are buying and from catalog sales that are usually from large companies with a reputation built up over time. The cost of doing sales in other ways tends to drive out the outright fraudsters.

2.7.3.3 eBay fraud examples

eBay is a Web-based auction house (for lack of a better term). But unlike a physical auction, people are not present, so the virtual nature of the venue leads to any number of frauds. Many sellers sell legitimate goods on eBay, but it's also easy to submit an item for sale at a low price, demand payment in advance, and not provide any goods. The next step up from that is to provide poor quality goods.

Anyone can also offer stolen goods, and eBay is certainly an opportunity to fence stolen goods that far exceeds most other opportunities a thief may find. Many low-cost goods are available and nobody seems to check for thefts on eBay goods.

The approach put forth by eBay to defeating these efforts is to associate reputations with sellers, but the seller reputation system has big problems. For example, many fraud groups create new sellers with no reputation, generate claims from fictitious people to build up a great reputation over a period of a few months, then start selling like mad for a few weeks, bringing in tens of thousands of dollars, not fulfilling, and walking away with the money, or fulfilling poorly and keeping a good reputation for some time.

As an aside, I am not picking on eBay. The fact is, they are dominant in this particular aspect of the Internet and they are exploited in this way far more than any other site in the Internet.

2.7.3.4 Nearly the same name

One of the favorite scams of fraudsters is to create a Web site with almost the same name as a real site and make it look like the real site. This sort of site can be used to pick up people who have made typos or other mistakes and to then create fraudulent schemes of all sorts usurping the trust they have in the brand name. Imagine a site called IBM.net or whitehouse.com taking over all of the attempted connects to IBM or the White House. Of course there is a whitehouse.com. It is a pornography site. Which leads me to a story...

Some years back, a secretary I knew at a government site was trying to get information from the White House Web site and accidentally entered ".com" instead of ".gov". Because the rules are so strict in government, she was really scared that she would be fired for it. The site kept popping up windows and she could not get it off of her screen. She was not fired because the management was reasonable, but this sort of fear can lead to exploitation.

2.7.3.5 Redirection and tunneling sites

Sites often capture the user within them. Then, within subwindows or through proxy mechanisms, they provide connectivity to other sites. Along the way they collect details of the interactions, perhaps redirect specific items to their versions, take credit card and banking information, and make it appear as if they were not interfering at all.

2.7.3.6 Online gambling sites

Online gambling sites are a potentially serious problem, especially for gambling addicts. There are several obvious problems.

2.7.3.6.1 The trust issue

How can you trust an Internet site to deliver random numbers, properly deal cards, not reveal information to other players about your cards, and spin dice fairly? It's not like Las Vegas where there is a gambling commission with investigative powers and real enforcement. Since it is illegal in most countries, most sites are run from foreign countries and the players are already breaking the law.

2.7.3.6.2 Isn't the lottery gambling?

The lotteries may be fair and you may some day be able to buy tickets to them online, but there are enormous problems because buyers have to trust computers in the Internet in order to guarantee that they are actually communicating directly to the lottery site. Others could intercept and change things along the way.

2.7.3.6.3 Online poker sites for free

There are of course free gambling sites where you can either make your own side bets not involving them or play Poker with the stars. But why would someone give you something for nothing? Isn't it obvious? They at least sell you things along the way, and depending on who they are, may offer additional services for fees or otherwise take advantage of you. Sure, some are legitimate sites that teach you how to play a game that is fun and only make money by selling you cards or equipment for your hobby. But is it really worth the risk?

2.7.3.7 Web sites to plant spyware

Many Web sites are used by fraudsters and intelligence gatherers to plant spyware in computers of those who visit them. This comes in the form of downloads that violate security of the system accessing the Web site (your computer). They usually exploit weaknesses in Web browsers or the programs that those browsers use to process incoming information.

2.7.4 Spyware, adware, and Trojans

Spyware is computer software that gathers and sends information about the computer's user and data to the people who sent out the spyware or their designee. The term spyware is also closely associated with adware, software that causes advertisements to appear on the target's computer, and the more general class of software that has hidden functions, so called Trojan horses.

2.7.4.1 Common spyware

Common spyware is the sort of thing that users of Windows-based computers get all the time. They collect keystrokes, Web site visits, data used to fill in forms, and other similar data and send it out using tricks of various sorts to the folks who collect the data and use it to take advantage in one way or the other. Examples of what they do with the data when collected are included here.

2.7.4.1.1 Credit card information

Use credit card information to steal goods and services leaving the bill with the original cardholder and their credit card company.

2.7.4.1.2 Identity information

Use identity information to forge identities and steal any number of things. In some cases this is used for identity theft, the worst case scenario for the individual who then takes a year to more to clear up their financial mess and reputation.

2.7.4.1.3 Information to send you more spam

Use information on Web site visits to trigger spam and other sorts of activities.

2.7.4.1.4 Resale of your information

Gather data about the people for sale to others, who pay for mailing list names to send more spam, information to commit more frauds, and so forth.

2.7.4.2 Adware

Adware is software that produces pop-up advertisements or alters Web browser settings to flood the target with advertisements. This can become obnoxious as well as leading to slowing of the computer.

2.7.4.3 Trojan horses

Most of the examples above use Trojan horses to do their dirty work. A Trojan horse is a program that performs a secret function. Trojan horses have been around since... Troy! And in all of the time between then and now, no solution has been found to this problem that can be applied successfully to most modern computers. If only I had the patent rights...

Trojan horses have been used for the widest range of applications, from gathering intelligence to causing computer crashes to stealing money to sending abusive messages to individuals. Today they are left in computers after break-ins so these computers can be used for other nefarious purposes, like attacking other computers, sending spam, creating a phony Web site, and... you get the idea.

2.7.4.4 Real spyware

Real spies - intelligence operatives - have long used Trojan horses to collect information, and of course they still do. Two of the more famous cases are included here.

2.7.4.4.1 The CIA source code theft scandal

The US CIA used the source code from a private company to introduce a Trojan horse into the Australian government taxation system, allowing the CIA to gain access to all of the financial and tax information over a period of years. Sadly, they didn't bother to tell the company that originally made the software who eventually got a service call from the Australian government. The CIA lost the law suit for copyright infringement and had their operation blown.

2.7.4.4.2 The Russian classified information Trojan

Somebody knows for sure but isn't talking about the case where the Russians apparently planted a Trojan horse in a printer driver for a classified system used by the United States. Somehow, that printer driver was able to release classified information over the Internet to a location in Russia for periods of months or longer. The US government does not deny this and it appeared in the newspapers in the late 1990s. But who knows?

2.7.4.4.3 Professionals use Trojans

Professional spies and operatives plant all sorts of hardware and software in systems and locations in order to gain ongoing access to information and capabilities for exploitation on command.

2.7.5 Child exploitation on the Internet

I have discussed with disgust some of the parts of this hideous and heinous crime that uses fraud techniques to gain access to children for exploitive purposes, but it is important to put it all together here. A lot of different people exploit children, from parents through slave traders. They include many common themes.

2.7.5.1 Custody battles

Separated, divorced, or otherwise estranged parents are sometimes involved in kidnapping children or using children against their one-time spouse. In some cases this may involve issues related to previous child abuse or accusations of abuse, but it most often involves cases of custody. In these cases, the Internet is used to gain access to the child, to sway their viewpoints, to arrange times and places for covert meetings, and in some cases to do the preparation for a kidnapping.

2.7.5.2 Child pornographers

Child pornographers exploit children over the Internet for money. They gain photographs and movies of children in situations ranging from simple and relatively innocent nude pictures to real-time video feeds of children being gang raped by adults. Some of these operations produce millions of dollars in sales per month and involve sites all over the world. They take credit cards and track the behavior of their customers. They may also take this information and use it to extort further money from those who go to visit these sites, or simply charge their credit card to the limit. They know that few if any of the people involved want to call the police to report that they were buying illegal child pornography and got ripped off in the process.

2.7.5.3 Serial child rapists

Serial child rapists use the Internet to find and entice their victims into situations where they can be assaulted. In many cases this process involves a kidnapping - either temporarily or over an extended period of time. In some cases these children are also filmed for sale to pornographers, leased out to child pornographers for further exploitation, sold to others for similar purposes, or simply killed and thrown into woods or swamps to destroy the evidence.

2.7.5.4 Baby sellers

Baby sellers kidnap children and sell them either through pseudo-legal means into the adoption system or illegally to women who want to hold onto their boyfriend or husband by faking a pregnancy and, eventually, have to produce a baby. They use the Internet as part of their intelligence gathering to identify and locate families with recent births.

2.7.5.5 Slave traders

Slave traders kidnap children to sell as slaves. They use the Internet predominantly as a communications tool to allow them to buy and sell without physical contact.

2.7.5.6 Some news examples

Look at this news story:

> Of the 413 people arrested as part of the FBI's "Innocent Images" investigation since 1995, "only a handful have not been upper-middle-class, educated white men," said Special Agent Pete Gulotta who serves as the investigation's chief spokesman. "They're almost all white males between the ages of 25 and 45. We've had military officers with high clearances, pediatricians, lawyers, school principals, and tech executives," Gulotta said of those arrested under Innocent Images.
>
> Of those arrested, 337 have been convicted of online child pornography trafficking or using the Internet to solicit children for sex, Gulotta said. The investigation actually began in 1994, but was not publicly disclosed by the agency until the following year. The Innocent Images operation is aimed at "taking these people out before they strike," which is why agents frequently pose as youngsters in chat rooms, acting as bait for would-be child abusers, Gulotta said.
>
> The Innocent Images project was sparked by the disappearance, in 1993, of a 10-year-old boy from Brantwood, Maryland, Gulotta said. While the boy, George Burdinski, was never found, the FBI obtained information linking his disappearance to a network of online child pornography traffickers, he said.

And here's another case:

> Police say Arkansas man made an online deal to buy a little girl for sex.
> Memphis police arrested an Arkansas man this week whom authorities said came to Memphis hoping to buy an eight-year-old girl for sex -- a deal he made in an Internet chat room.
>
> Arlon Simpson, 50, a University of Arkansas custodian, allegedly made the request to a woman with whom he had been trading child pornography online. The woman then notified the police. "The [woman] had advised [police] that Simpson was wanting to purchase an eight-year-old girl to raise as his daughter and introduce her into a sexual relationship with him," said Joe Ball, an inspector at Shelby County Sheriff's Department, in Tennessee.
>
> The woman had ongoing Internet contact with Simpson, a Prairie Grove, Arkansas resident, since June for purposes of child pornography and other sexual reasons, police said. Using the woman as an undercover informant, police said they arranged for the sale of the girl. The deal involved the woman stating that she had a fictitious niece named "Stacey" whom she would sell to Simpson for $500, police said, but the price was too steep for Simpson.
>
> "Mr. Simpson balked and stated that he only had $100," Ball said, "and would exchange numerous compact discs loaded with pornography, and numerous hard copies of child pornography for the remainder of the money."
>
> Police said that Simpson traveled from Arkansas to Memphis, hoping to pay for the young girl but the sheriff's department was waiting for him. Simpson was arrested Saturday afternoon in the parking lot of a Wendy's fast-food restaurant in east Memphis.
>
> When they found him, police say he had a loaded gun, a teddy bear, and child pornography. Simpson is charged with aggravated sexual exploitation of a child and unlawful possession of a weapon and is being held on a $10,000 bond. Currently, Simpson faces only state charges, however, the US attorney's office says it is reviewing the case.

Clearly we have to protect our children from these criminals, but how can we do it? I'll discuss this later.

2.7.6 All source intelligence and the Internet

In the many demonstrations I have done of penetration into all sorts of enterprises, one of the most compelling things that my teams do is use information posted to the Internet to gather intelligence on our clients for exploitation later in the red teaming process.

2.7.6.1 Red teaming

Red teaming comes from military strategic scenario games in which groups of people are put on different teams in order to gain understanding of how attacks might take place and how defenses might be built to defeat those attacks. This methodology produced examples like running planes into buildings and stadiums long before Bin Laden ever came up with the idea, regardless of what government officials may have their citizens think.

2.7.6.2 What and where on the Internet

Among the red teaming methodologies that I have taught and used, is the notion of the use of all source intelligence - intelligence gathered from all sources and applied in concert to understand the situation. In my experience, mailing lists are one of the best sources of this sort of intelligence available over the Internet and one of its most useful purposes. To most people, these things are trivia, but to the skilled operative, they are like little chunks of gold that can be collected and used.

2.7.6.3 Job postings

They find job postings and use them to understand how to penetrate the organization and what sorts of systems and projects they are working on. This helps to create frauds like the copier frauds described above by giving information on what sort of equipment the fraudster will claim to be maintaining today.

2.7.6.4 Postings to professional lists

They find postings to professional lists and use them to understand what individuals within companies are working on and what sorts of problems they are having with their work. Use this to sell them custom solutions in just the area they are looking for.

2.7.6.5 Where who will be

They find out from announcements where individuals will be appearing and exploit it for stalking them.

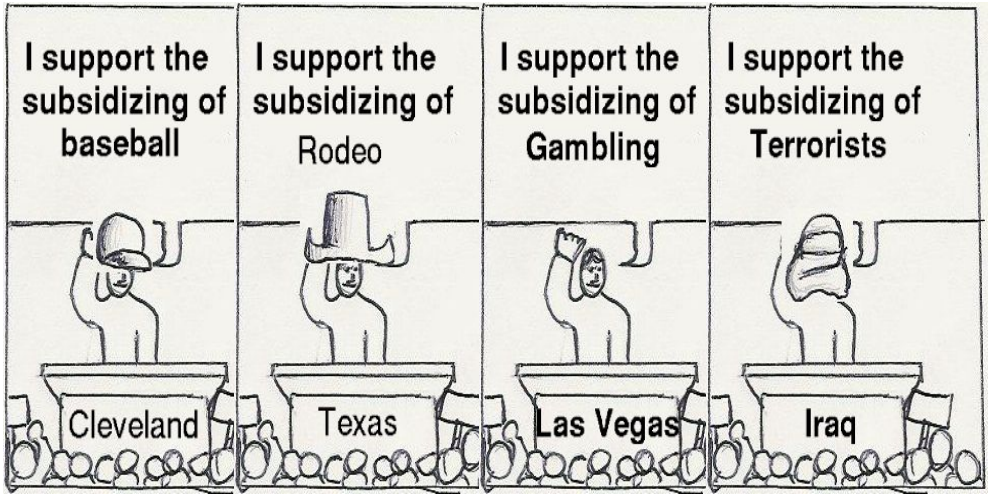
2.7.6.6 Financial information

They find detailed breakdowns of sales, profits, and so forth from presentations sent to mailing lists associated with conferences or shareholder meetings.

2.7.6.7 Locations and facilities

They find extensive information on locations of the company and what those locations are used for to allow the proper location to be approached.

2.8 Politicians and their parties



Politicians and political parties are among the most skilled groups at taking by lying that can be found anywhere. And they do most of it legally, perhaps because they get to set the laws and help determine how they are enforced.

2.8.1 The ones that get caught

It's not hard to show that politicians are more likely to commit frauds than the general population. All you have to do is count the ones that are convicted. But if you did this you would be missing a lot.

2.8.2 The ones that slide by

Politicians have a lot of ways of using the laws they put in place to their advantage. Here are some of the widely known areas of political benefits. Just remember, it's your money they are taking.

2.8.2.1 Pork

Pork barrel politics is the norm in the US. The party in power funds projects in the states that will help them get re-elected, or at the state and local level, the districts, counties, and cities where they got funding or need votes. Put a military base up here, build another highway there, and you feed the economic well being of the folks who voted for you while systematically moving that money away from those who voted against you. It's perfectly legal.

2.8.2.2 Taxes

Did I mention that they are taking this money from you and me? Yes, that's right. They send in the tax collector to force you to give them money to spend on things you don't want. It's called redistribution of wealth. Of course we all tacitly agree to this by remaining here. We could go somewhere else where they tax more or less and provide more or less or different government services.

2.8.2.3 Land grabs

The US Supreme Court recently ruled that eminent domain laws allow government to take land from you and give it to someone else so they can make more money with it. This is just the latest in a series of breakthroughs in the eternal land grab scheme.

2.8.3 Campaigns

But the biggest of the biggest frauds of all time are the promises we get in political campaigns. They range from outright lies to the subtle techniques like push polling. While not a political analyst, I figure I might as well point out these issues. Political campaigns are cases where the politician gets something substantial (elected, power, position, title, influence, money for their friends and family, etc.) by telling the public things that are not strictly (or often even loosely) true. In other words, lies or deceit. So at least by my definition, whether illegal or not, politics seems to have a lot of fraud. But we will give them a break and just call them lies.

2.8.3.1 Lies about themselves

In the US, many politicians seem to come from poor families and have worked themselves up from dirt. In fact most of their personal stories are pretty close to true. But when it comes to military service, plenty of folks embellish either directly or by inference. Think George W. Bush and the carrier. He is in an air force pilot's uniform as if he landed on the carrier when in fact he was a pilot in the national guard during Viet Nam but never flew onto a carrier or anywhere near combat. It's a subtle sort of lie. Not like Clinton who faced a camera on national television and told the nation that he never had "sexual relations" with that woman. Of course who knew that "sexual relations" didn't include the kind of sexual relationship he had with that same woman. It's another outright lie. And lest we

forget, neither of these folks were the fist US presidents to be caught in lies. And of course the President is the top politician, just imagine what other politicians are doing. I guess you really don't have to imagine. They seem to get called on lots of lies and yet they get away with many of them too.

2.8.3.2 Lies about the other guys

But the lies about their own purity, skill, and wonderfulness hardly compare to the lies about the other guys. Here is where politicians really excel. Many campaigns sound predominantly like "Do you still beat your wife?". Who can forget the advertisements identifying opponents as soft on crime because the opponent was governor when a future killer was let out of prison?

2.8.3.3 Push polling

And whoever thought of so-called push polling was a political genius (real fraudster). In this scam, the supposed pollster asks a leading question like: "If Murphy admitted that he sent millions of your tax dollars to his best friend in low interest loans that were never paid back, how would you vote on his election run for governor?" The notion that it's a poll is a lie, and the premise is also a sort of a lie... “I said if...”.

2.8.3.4 Lies about who's telling the lies

But of course they have turned the lies about who is telling the lies into the biggest lie of all. It's practically a science. "That was a commercial put on by the organization to re-elect the president, an organization over which we have no control." Right. Like the President knows nothing of the groups that are run by their just departed chief of staff. And these days we get the really radical ones like "MoveOn.org" and "Swiftboat Captains Against Kerry". The candidates deny involvement while cheering them on.

2.8.3.5 Lies about the crowds

And my favorite before going on to another subject area, the lies about the crowds. The Bush presidency has been more effective than most at this one, but all candidates seem to try it. In this sleazy move, the crowds at events where the politician speaks are selected from among their biggest fans. Whether the military members selected to ask questions in front of the press are told

what to ask or the protesters are kept 4 blocks away from the speech with police barricades, it's all the same. And of course crowds of 50 are made to look like 5,000 by camera angle and field of view selection.

2.8.4 Propaganda

Politicians and political parties are ultimately in control of the state communications means and this implies the capacity to control what the public sees to a substantial extent. Propaganda is perhaps the largest scale and most harmful sort of deception used on populations. I won't spend a lot of time, but I think it is worth studying the issues of propaganda from at least a few perspectives; Hitler in World War 2, the "War i$ $ell" video, and others.

2.8.4.1 What is propaganda?

According to dicitonary.reference.com:

> *"The systematic propagation of a doctrine or cause or of information reflecting the views and interests of those advocating such a doctrine or cause."*

Wokopedia.com says this:

> *"Information specially designed to make people feel a particular way or believe a particular thing."*

Webster's dictionary says:

> *"The spreading of ideas, information, or rumor for the purpose of helping or injuring an institution, a cause, or a person"*
>
> *Ideas, facts, or allegations spread deliberately to further one's cause or to damage an opposing cause; also : a public action having such an effect"*

I'll buy into these.

2.8.4.2 Hitler's propaganda machine

Hitler's Germany built up one of the most powerful and horrific propaganda machines in modern times. The Crusaders brought many people far from their homes to kill other people with almost identical beliefs, but Hitler's propaganda machine created levels of hatred never before achieved. My coverage is pathetic, but my objective is not to document the incidents. It is to point out examples of propaganda then and now.

2.8.4.2.1 Crystalnacht - the people have spoken

The night of broken glass was the night that Hitler's thugs solidified their power over the people by instilling fear and unification around the Jewish threat to the German people. This is a form of propaganda that creates the self fulfilling prophecy. Hitler talks about how the people must act to retain their own best interest, and the people seemingly act, all on their own. Of course it was orchestrated, but Hitler actually disassociated himself from it while declaring it as a sign of what the people believed.

2.8.4.2.2 Gypsies and Jews - the common enemy

The Gypsies and Jews were blamed for the trouble of Germany. It is a popular approach, creating the common enemy. I have a saying that when people in government start to blame the Gypsies and Jews, the society is preparing for a revolution. Unite against them and you are united. Propaganda creates fear of an identified enemy and the country unites behind the enemy's defeat and the leadership who points it out.

2.8.4.2.3 Less than human - beauty

Dehumanizing the enemy is necessary in order to convince normal people to kill them and take everything they own without feeling guilty. Hitler's regime was a standout in dehumanizing other people. The purity of the German race and the impurity and obvious physical characteristics of others was a defining feature of the Hitler propaganda based on beauty. The eyes of the beholder are always shaded when put in the context of their own characteristics as beauty and others as ugly.

2.8.4.2.4 We are the oppressed

Hitler was also very good at pointing out that the German people were oppressed and that they should be leading the world. Of course they were oppressing record numbers of people as slaves and killing millions in their way, but they were always surrounded by the impure oppressors who were keeping them from their rightful place in the world and hemming them in.

2.8.4.2.5 Euphemisms – the final solution

It's not genocide, it's the final solution! Killing the disease that is destroying the purity of our race. That was the propaganda.

2.8.4.2.6 Stay the course - we are wining

Up until the day he killed himself, Hitler maintained a positive attitude and projected this to his people. He told them they were winning even as Berlin was being bombed almost out of existence. They were always winning, and nobody was available to ask what exactly losing would look like if this was winning.

2.8.4.2.7 Afterlife

And in the end, even with Hitler dead and many years gone by, the lingering effects of Hitler's propaganda remain in the minds and views of the remaining Nazi groups around the world. This shows just how pernicious a propaganda machine can be.

2.8.4.3 War i$ $ell

Brian Standing recently released his video titled "War i$ $ell" which describes the propaganda associated with war throughout history and with images, pictures, and all manner of other examples. It is very informative and thought provoking and worth getting. Here's my take.

2.8.4.3.1 Demonize the enemy

A great example is the story about the first Gulf war when the Iraqis were accused of removing babies from incubators and letting them die on the floors of hospitals. It was a lie according to the doctors in the hospitals. But it was repeated by US senators, the President (Bush 1), and others, and was a rallying point for demonizing the Iraqis and increasing the urgency of going to war.

In most wars a name is given to the enemy that makes them seem less human. "Gooks" from the War in Viet Nam, "Huns" from World War 1, and so on. It's a lot easier to kill people when you don't think of them as people. They are just demons.

2.8.4.3.2 Get third party endorsements

The news media is the best so-called independent source of information. It turns out that almost half of all the news on the news is actually public relations given to the media by advertisers and other similar interests. And of course every public relations firm helps inform the media so that their clients can get the advantage of the newspaper endorsement in the form of writing the story.

Public relations work for everyone. Even I use it to generate sales of my books. Without it you would never know of this book. (If you are from the media, no offense... I am available for interviews...)

2.8.4.3.2.1 News endorsements and better

Propaganda uses media in this way all the time and to great effect. And in countries without alternative media, where the government controls the media, propaganda can be even more effective. However, in most such places the people recognize that the media is government controlled and this limits its effect. What is far worse is controlled media in places like the US where there is substantial control on select issues, but the media appears to be independent. We then get “fair and balanced” propaganda which has the benefit of endorsement without the taint of government control.

2.8.4.3.2.2 Hollywood endorsements

Another major third party sought as part of government propaganda is Hollywood and the movie industry. Anybody who claims that the Hollywood media is somehow left wing is missing all of the movies made by Hollywood in support of every war the US has ever been in, including the ones in Iraq.

2.8.4.3.2.3 Educational endorsements

The use of the educational system as a tool for propaganda is incredibly effective and nowhere is this better demonstrated than in the Middle East where some Arab countries educate their students to hate Jews. This was done by Hitler and produced a long legacy of problems for Germans. It is moving in on the third and fourth generation of Arabs and is producing incredible problems for them in their own countries as well as in the rest of the world.

2.8.4.3.2.4 Religious endorsements

In many societies, endorsement of religious leaders is critical to any successful propaganda campaign. In the US, churches seem to break the law in terms of separation of church and state by getting involved in political campaigns, but no politician can oppose them without enormous backlash. And yet the US is a piker in religious endorsement compared to its role in the Arab conflict with Israel. In Rome, without the Pope behind it, you are unlikely to sway many folks either. Theocracy is alive and well and living covertly in modern societies.

2.8.4.3.2.5 Funding endorsements

When the sources of money become endorsements for views, even science starts to break down. Funding sources are pressured by political groups, organized boycotts, write-in campaigns, and political or religious beliefs to the point where certain sorts of science are not permitted on grounds unrelated to scientific validity. Of course the experiments on humans done by Hitler's Germany were of scientific value even though most people all around the world find them abhorrent. When politics creates propaganda surrounding science and uses funding to gain control over who in the research community can say what, the endorsement no longer benefits society and the people.

2.8.4.3.3 Use branding

The idea of branding is to stamp sayings in the mind of the targets. For example, linking support for a war to freedom and democracy even if the war is not about that at all. The portrayal of the political system as a sort of religion is part of the dogma. And in order to be effective, propaganda has to be put in the target's terms. It has to be believable at the time it is received, given at a receptive time, and targeted to the audience. Consider the "*War on Terrorism*" turned into name after name after name until today it is... actually it is still changing....

2.8.4.3.4 Stay on message

This is done as a form of scripting. Standard answers are given to questions and any question that is not aligned to a standard answer is twisted in the response toward a standard one. Key phrases are repeated - often word for word - by all of the members of the propaganda team.

2.8.4.3.5 Tell "the big lie"

The big lie is the lie told by people in a position of authority as if it were fact when it is in fact a lie. If they repeat the lie enough times, are in authority, are trusted, and go relatively unopposed, the lie will become a social truth and be treated as fact. How many times did we hear that there was no question the Iraqis had weapons of Mass Destruction? Who tells the big lie? Whoever is in power! Nobody else can!! They would if they could.

2.8.4.3.6 Use doublespeak

Phrases like the "axis of evil" are outstanding examples of wording that implies both the evil group of enemies in World War 2 and the notion that the countries listed are somehow working together even if they are not.

2.8.4.3.7 Silence the opposition

A key factor in success is reducing the amount of resistance shown by anyone who opposes the message of the propagandist. For example, war propagandists attack pacifists by saying that they are doing nothing while evil flourishes. The phrase "If you aren't with us, you are against us" is intended to quell any contradictory views. The notion of the loyal opposition is lost, which often leads to catastrophic failures. If you are against the war, you are against democracy. Plug in your religion, political system, or other “ism” and it works just as well.

2.8.4.3.7.1 Don't let them come to the table

Another set of tactics to silence opposition is to not invite them to conferences, keep them off of the television, and generally keep them from being in the know. This uses the power of position in its influence on access to information.

2.8.4.3.7.2 Don't fund their science, fund yours

The use of funding of research is an extremely powerful tool of propaganda. In essence, you can silence the opposition by not funding those who disagree with the official position. You can also fund those who favor it. Biased research is often ferreted out by the scientific process over time, but from the view of the propagandist, they don't need to win forever, just long enough to have their fait-a-complit. You can't go back now!

2.8.4.3.7.3 The chilling effect

The chilling effect happens when people are directly or indirectly threatened by what they see around them. They decide to stay quiet rather than risk becoming the target of the propaganda campaign. Think of the McCarthy era in the US and its ability to silence any opposing political views under the taint of communism. And think of how many scientists will continue to speak of global warming if it results in them being defunded and fired.

3 Understanding Deception

At the heart of frauds are deceptions, and this chapter is about deceptions and how and why they work. The reader not interested in technical details may skip this chapter... at their own peril.

Many others have contributed to this part of this book through their earlier work with me. Special thanks go to Charles Preston, Eric Thomas, Deanna Koike, Irwin and Jeanne Marin, Fred Feer, Garrett Gee, Anthony Carathimas, and Dave Lambert for their outstanding efforts in this area.

3.1 Definitions

There is a lot of detailed literature on deception and the issues have been long understood and applied by many people. According to the American Heritage Dictionary of the English Language (1981):

"deception" is defined as "the act of deceit"
"deceit" is defined as "deception".

Even the definition of deception is deceptive.

Since long before 800 B.C. when Sun Tzu wrote "*The Art of War*", deception has been key to success in warfare. The practitioner of deception utilizes the target's intelligence and information sources to convey a deceptive signature of the desired impression. The deception takes place in the mind of the perceiver. That is:

> Fundamentally, deception is about exploiting errors in the target's cognitive systems for advantage.

So in order to understand how deception works we really need to understand the kinds of mistakes people make, and in order to counter deception, we need to understand how to prevent those mistakes from being made or detect and react to mistakes in a time frame and manner that prevents the harm.

3.2 People make lots of mistakes

It turns out there are a lot of different ways that people make mistakes, and the psychologists of the world have spent a lot of time figuring them out for us.

3.3 Easily fooled

According to Bob Fellows ("*Easily Fooled*", Mind Matters, PO Box 16557, Minneapolis, MN 55416, 2000) the following characteristics improve the chances of being fooled:

- Stress
- Naivety or Idealism
- Life transitions
- Unfulfilled desire for spiritual meaning
- Tendencies toward dependency
- Attracted to trance-like states of mind
- Lack of assertiveness
- Unaware of how groups can manipulate people
- Gullible
- A recent traumatic experience
- Want simple answers to complex questions
- Unaware of how the mind and body affect each other
- Lack critical thinking skills
- Disillusioned with the world or their culture
- Lack knowledge of deception methods.

Fellows also identifies a set of methods used to manipulate people.

3.4 How we know

Thomas Gilovich ("*How We Know What Isn't So: The fallibility of human reason in everyday life*", Free Press, NY, 1991) provides in-depth analysis of human reasoning fallibility. This includes notions that people (erroneously):

(1) believe that effects should resemble their causes
(2) misperceive random events
(3) misinterpret incomplete or unrepresentative data
(4) use their biases to shade ambiguous and inconsistent data
(5) have motivational determinants of belief
(6) bias second hand information, and
(7) have exaggerated impressions of social support.

3.4.1 Effects should resemble their cause fallacies

The notion seems logical and yet it is generally not so.

3.4.1.1 Instances should resemble their categories

Similar looking animals must be more closely related genetically than different looking ones. Of course this is not true.

3.4.1.2 Like resembles like

Measles come from germs with spotted coatings. Of course this is not true either.

3.4.2 Tendency toward oversimplification

If it looks like a duck and quacks like a duck, it must be a duck. That's what the ducks who get shot by the hunters seem to think when faced with decoys. Think through the frauds described earlier and you will find many of them involve dressing the part and talking the talk.

3.4.2.1 Occum's Razor

When a simple explanation will do, choose it over the more complicated one. When the fraudster tells a tale, there is a tendency for it to seem logical if you don't think about it too much and it is usually pretty simple, even if couched in a good story.

3.4.2.2 Black and White

People tend to prefer simple definitive answers over ones that have shades of gray. Of course things are often more complex, and thus the tendency for sound bites to dominate the media and the political decision process in most modern societies.

3.4.2.3 Rule of 3s

Lists of three things are better accepted in some cultures. There are three reasons for this; (1) the cultures have literature including religious texts going back millennia that support these numbers, (2) it is embedded in their implementation of automated tools such as computerized slide generation systems, and (3) it is linked to memory retention capabilities that limit the number of simultaneous thoughts to ... just kidding, this list of three things was just an example of how lists of three things seem like they make sense.

3.4.3 The misperception of random events

Many people don't understand enough about statistics to even analyze this issue clearly, and of course most never go to that depth of thought about issues. Always question statistics.

3.4.3.1 The clustering illusion

Events appear to be correlated even when they are not correlated. For example, cars traveling on highways tend to cluster because faster cars slow down behind slower ones. This produces clustering even if desired driver speeds are quite different.

3.4.3.2 Over application of representativeness

The “law of small numbers” states that a few examples are taken as more significant than they really are from a statistical point of view. Thus we see what is called evidence in the form of an example or two in many political speeches. Bill Gates never graduated from college but is the richest man on Earth. But the next 99 of the richest 100 did go to college and almost all of them have post graduate degrees. Education correlates very strongly with financial success in Western societies.

3.4.3.3 Misperceptions of random dispersions

Random events are seen as "shooting streaks" because randomness is not well understood by most observers. When statistically analyzed, most shooting streaks are well within the normal variation of the player's normal performance levels.

3.4.3.4 The creation of causal theories

People have a tendency to create theories to explain what they see, and adopt them regardless of evidence. Fraudsters take advantage of this by creating a casual theory that the person looking for hope can embrace.

3.4.3.5 The regression fallacy

People underestimate the effect of regression. For example, if you usually average two sales a day and make five sales for each of three days in a row, people will think you are in a slump when you only make one or two sales a day for the next week.

3.4.4 Incomplete or inadequate data misinterpretation

Most frauds involve incomplete information.

3.4.4.1 The excessive impact of confirmatory information

A small number of confirmations are treated as proof, while an occasional refutation may be dismissed as invalid for some after-the-fact reason. God will see you through. See, you are still here. I must be right! Fraudsters use this all the time by creating their own confirmations in the form of a shill.

3.4.4.2 The tendency to seek confirmatory data,

If you are looking for red in fires you will tend to count orange as red, and not discount the presence of blue along with red. If you are looking for salvation, a fraudster may appear to be that salvation and you will tend to ignore the imperfections in their fraud.

3.4.4.3 The problem of hidden or absent data

If you justify the quality of your hiring process by tracking only the success rates of people you hire, you are ignoring the missing data on how successful the people you didn't hire might have been. One of the most interesting frauds uses this to the advantage of the fraudster by claiming to be able to predict if a stock will go up or down on a daily basis. The first day they send our 64 letters, half saying the stock will go up, the other half saying it will go down. Depending on the outcome they will send 32 letters the next day to the ones that they got right, half claiming another stock will go up, the other half claiming it will go down. Next day 16, next day 8, and finally for the 6th time in a row, they picked the right stock going the right direction for the 4 remaining people. From the point of view of those 4 people the fraudster must be the world's greatest stock broker - time to invest.

3.4.4.4 Self-fulfilling prophecies

If people believe the markets are crashing, they will pull their money out, and thus the markets will crash. If you believe in salvation, I can salvage you. Ponzi schemes are a great example of these prophecies - for a little while.

3.4.5 Bias laid on ambiguous and inconsistent data

Some data is just not good enough to make a determination about something. But if you have a point of view, that same data can be used to support it. This is one of the major problems with political speech on the public airwaves today. A lack of a “truth squad” checking the facts and the adequacy of the evidence leads to all claims being presented as equal.

3.4.5.1 Ambiguous information is interpreted in context

We tend to interpret ambiguous data in the context of what we are looking for. For example, when you look at clouds and see shapes, they are not really those shapes, only clouds. When hungry, people tend to see food in those shapes. Vice President Cheney kept telling the media that the increase in attacks on US troops was a sign of desperation and indicated that the US was winning the conflict. Finally, after weeks, someone asked “If increased attacks on US troops is a sign of winning, what would be a sign of losing?”

3.4.5.2 Unambiguous data is shaded

An explanation for the invalidity of data that is inconsistent with theories is often found. This is common in scientific experiments as well as in frauds. And it is even more common in politics. The fact that exit polls in a few specific locations in Florida differed significantly from the final vote counts led the media to predict that Bush would lose his Presidential election run against Gore. In the media republican pundits claimed that the difference was because voters didn't want to admit that they voted for Bush. But everywhere else the exit polls were consistent with the vote counts. In electronic voting systems without proper records, the only indication of fraud is the difference between exit polls and vote counts.

3.4.5.3 Multiple endpoints

If the data is ambiguous we will tend to associate it with our expectations for outcomes, thus biasing the result. For example, some element of a baby's face looks like anyone and will be associated with the parent's face even if the child is adopted. Just think of how flattering you can be this way.

3.4.5.4 Confirmations and non-confirmations

Non confirmations are often ignored rather than treated as refutations. Selective memory is an example where people will tend to remember predictions that come true over time and forget those that do not come true. Fraudsters try not to get so deeply involved that they have to deal with this issue, however, they do deal with it in cases like fortune tellers and similar long-term operations.

3.4.5.5 Focused and unfocused expectations

If we believe that bad things come together in threes but don't set a time limit on what it is to come together, we will wait till the count hits three and declare that we were right. If we are trying to associate a dream of a sunny day with events of the day, we will find the moment that the sun broke through the clouds as a confirmation. These sorts of phenomena are often exploited in the fortune telling and wise person frauds. The lack of a time frame is particularly useful for predicting the end of the world. Here is my prediction for you: "Terrible news is coming your way, but you will overcome your grief and prosper if you stay focused on what is important." That will be $50, and I want you to come back next Tuesday at 2PM, not a moment late, and tell me what happened this week. I will be praying for you. Of course when you come back and nothing has happened, I have a line for that one as well: "Thank God it worked. I prayed all week for you and made an offering at the Gypsy Temple for $10 each day. Thank God the tragedy was averted. The coming week will see you prosper. That will be $100 (I have to cover my donation expenses after all).

3.4.5.6 Outcome asymmetries and one-sided events

These include four types of asymmetries; hedonic, pattern, definitional, and base rate asymmetries.

3.4.5.7 Hedonic asymmetries

There is a tendency to overemphasize things that are more striking to us. For example, it may seem like you almost always get splashed by a passing car on wet days, when in fact you just remember being splashed more than not being splashed. Again, this is great for making predictions and recalling commonalities.

3.4.5.8 Pattern asymmetries

You remember when you wake up and see 1:11 or 2:22 on the clock better than when you see 1:52 or 2:17. "Tell me when you awoke... 2:22 - the sign of the afterlife. Have you had any relatives die recently? Let's see if we can contact them - with your strong connection to the dead, we should be able to find a loved one that recently passed with relative ease." That will be $75 please. Afterlife tolls are getting higher and higher these days.

3.4.5.9 Definitional asymmetries

Things won't get better till you have hit rock bottom. But since “rock bottom” is not predefined, it is always able to be true since we can call wherever you turned around, rock bottom. Lots of these are useful for the prediction game.

3.4.5.10 Base rate departures

"Thinking about being healthy will help you cure cancer" is supported by people who have thought about being healthy and survived, but it ignores the people who thought about being healthy and died, because they are not available as data points.

3.4.6 Motivational determinants of belief

People who want to believe will believe and people who don't want to will not. Motivation drives belief.

3.4.6.1 Empirical support for the wish to believe

After the Nixon / Kennedy debates, supporters for each side thought their side had won. They interpreted the same thing in different ways. It's easy to defraud people who want to believe in things because they will interpret the fraudster as legitimate as long as the presentation matches expectations.

3.4.6.2 Mechanisms of self-serving beliefs

If you want to believe it you ask "Can I believe it" while if you don't want to believe it you ask "Must I believe it". As a result, preconceptions drive outcomes of belief systems.

3.4.6.3 Optimistic self-assessment

The vast majority of people believe they are above average in intelligence and beauty. To quote Garrison Keillor in his description of a small town called Lake Woebegone, MN, "Every child is above average". Given this context, it's easy to understand that, while some folks will fall for almost any fraud, smart people like us only fall for the top fraudsters.

3.4.7 The biasing effect of second hand information

Because so much information is second hand today, the way it is presented to us determines much of how we interpret it. Think in terms of the news media and how their take on things effects what the public perceives.

3.4.7.1 Sharpening and leveling

In relaying situational information, descriptions of peoples' behavior tends to be emphasized (sharpened), while descriptions of their surroundings tend to be deemphasized (leveled).

3.4.7.2 Corrupting effects of indirection in evidence

The game of “telephone” is a great example of this. As information goes from source to source and gets rewritten and re-described it tends to lose its fidelity then its integrity.

3.4.7.3 Telling a good story

In order to make the story interesting to the audience, distortions are often introduced. The “historical” movies that come out of Hollywood are examples of how telling a good story often distorts facts in favor of "flavor". Fraudsters are often very good at telling a compelling and believable story.

3.4.7.4 Distortions in the name of informativeness

Stories are often told with exaggerations of the fact to make a point. A little girl down the block did that and she was never seen again... Of course fraudsters almost always distort, but not to inform as much as to misdirect.

3.4.7.5 Distortions in the name of entertainment

“There is one example of...” becomes “I had a friend who...” and the audience misinterprets it as if their own friends probably... Inquiring minds want to know... The media is notorious for this.

3.4.7.6 Distortions in the name of self interest

Look at the statements of political parties and you cannot miss the distortions. Of course all sorts of fraudsters distort for self-interest.

3.4.7.7 Distortions due to plausibility

So-called urban legends are good examples of this. For example, the non-existent US patent agent who supposedly resigned because he thought that nothing else could be invented.

3.4.8 Exaggerated impressions of social support

Essentially all people think that they are right or justified and that the world knows it.

3.4.8.1 Social projection and the false consensus effect

Most people think that most other people agree with them about their views on things. Fraudsters leverage this by supporting the views of their targets to enamor themselves to their targets.

3.4.8.2 Inadequate feedback from others

People may agree out of politeness or not indicate that they disagree because of a desire not to offend. Children show less of this than adults and fraudsters show this at every turn to stay on the good side of their targets.

3.5 Distortions of information

Charles K. West ("*The Social and Psychological Distortion of Information*", Nelson-Hall, Chicago, 1981) describes the steps in psychological and social distortion of information and provides detailed support for the cognitive limits leading to deception.

Distortion comes from the facts that:

- A person can only perceive a limited number of events at any moment.
- A person's knowledge and emotions partially determine which of the events are noted and interpretations are made in terms of knowledge and emotion.
- Intentional bias occurs as a person consciously selects what will be communicated to others, and
- The receiver of information provided by others will have the same set of interpretations and sensory limitations.

3.6 Negotiations and influence

First Karrass ("*The Negotiating Game*", Thomas A. Crowell, New York, 1970.) then Cialdini ("*Influence: Science and Practice*", Allyn and Bacon, Boston, 2001.) have provided excellent summaries of negotiation strategies and the use of influence to gain advantage. Both also explain how to defend against influence tactics.

3.6.1 Reciprocation

Reciprocation is based on the notion that when you give something to me I will give something to you. Some of the well known and well confirmed examples are listed here. For fraudsters, this represents an opportunity to create an obligation in the target. Consider all of the fraud scenarios described above and you will find that many of them involve an apparent gift that creates an obligation which is returned in the form of trust. The trust comes in the form of who holds the money.

3.6.1.1 If it costs more it is worth more

Raising the price on many items increases their sales volume because the buyers are looking for high quality and associate it with price.

3.6.1.2 People tend to reciprocate any gifts

For example, even a meaningless gift will create an obligation. Refusal to accept a return gift makes you less likable because of the lack of opportunity to reciprocate. This is the reason that people who work for the Federal government cannot accept gifts. Because, even if they don't want to be biased, the gift biases them subconsciously.

3.6.2 Authority

People tend to use authority as a substitute for understanding or thinking. Here are the mechanisms.

3.6.2.1 Experts know more than others

When someone believes you are an expert, they will tend to defer to your opinions regardless of the sensibility of those opinions. This is reflected in the manner in which people are introduced in all sorts of settings, and most fraudsters create introductions for themselves as the first step in their person-to-person frauds. Examine the fraud

methods described earlier and see how many examples there are of shills and fraudsters using fictitious credentials. It's fairly dominant.

3.6.2.2 Duty to authority is deeply embedded in culture

Higher authorities overrides lower ones, appearance of authority replaces real authority, titles lead to the appearance of authority, and there is higher deference to known authorities. Fraudsters often use the color of authority to carry out their activities. Most of the organizational person-to-person frauds involve this element.

3.6.2.3 Appearances imply authority

Higher position appears to be taller, taller is projected as more important, importance is seen as larger, larger size implies more strength. clothing and accouterments imply authority (as a function of situation), and other trappings imply authority. Obviously this did not apply to Napoleon, but in most cases, the presentations by fraudsters are designed to exploit this mechanism in order to avoid being challenged. They “dress for success.” That's why the computer repair, cash drawer auditor, bank examiner, and so many other frauds work so well. There is an expectation of appearance and demeanor that the fraudster fulfills by their attire and behavior. The employee who challenges this risks offending someone important. Unless the environment supports challenges to people dressed like executives, the employee is likely to comply with requests.

3.6.3 Contrast

Substantial differences tend to be exaggerated and many things are taken relative to context. After having your hand in hot water, luke-warm water seems cool. To sell something expensive, you might start by offering something more expensive and work your way down. Looking at gasoline prices in the 2003-2005 time frame, the prices doubled, but when they went down by ten percent it was projected and believed as a "whew - things are getting better" sort of thing by many. As a strategy, going further and backing down more slowly was identified by Karrass as a critical negotiation tactic. For the leaders of negotiation teams for countries all around the world, this has become standard fare. What shape will the table be? Where will everyone sit? These take weeks or longer to settle before the actual negotiations even start.

3.6.4 Automaticity

Certain things are just automatic in the way people interpret the world around them.

3.6.4.1 Because

When you add a “because” followed by no new information, the chances of compliance increase substantially. This is because people tend to believe things when described this way. OK - that was an example. The notion that there is a cause and effect relationship leads to the notion that there is a reason, no matter how irrelevant the supposed reason is. A famous saying goes "Post hoc ergo proctor hoc." which means before, therefore because. But ordering does not imply causality because... OK you have had enough of this by now.

3.6.4.2 Desire not to think

Most people do not like to think. If it requires thinking and the target can back down to a simple rule of behavior, they will try to do so. This is often taken advantage of in the use of things like the "because" clause. Because they don't want to think and the "because" makes it seem like the speaker thought it through, they can simply take it for granted that the cause is as described and accept it more easily. Think about it!

3.6.4.3 Strong desire not to rethink

If it requires rethinking, it introduces self-doubt, and this will be avoided unless absolutely necessary because it affects the target's ego to imagine that they could have been wrong. Actually, that was a because that I cannot really justify, but I used it because we are in this section and I thought it would be convincing. Of course you could rethink this whole thing, but then that would be too hard, so just move on.

3.6.4.4 Default decision process

Logic is only used if there is a desire and ability to analyze the situation. Otherwise, pattern matching to known social behavioral patterns is used. This is part of a general theme in the way people act. If you say "Hi, how are you?" someone will likely say something like "Fine, and you?". A good example of this comes from Karrass who indicates that once people start to make little agreements, “yes, yes, yes”, they become more likely to say yes again and again. If you've done it before it must be alright to do it again. If those around you are doing it, it must be alright for you to do it too. Like lemmings to the sea.

3.6.4.5 Enhancement of automaticity

Automaticity can be enhanced by increased amounts of rush, stress, uncertainty, indifference, distraction, and fatigue. By adding to these elements to a situation, fraudsters can often drive behaviors of their targets toward their desired actions. The fraudsters know to use this to increase their effectiveness.

3.6.5 Reciprocation and contrast together

“Reject and retreat” is the name of a strategy that invokes both reciprocation and contrast. The fraudster starts by asking for a lot, but then lowers the request to something smaller. By reducing the request, the fraudster gives a concession (reciprocation leading the target to offer something). By lowering from a higher value, the fraudster invoked contrast (the second request doesn't look as big). If this is done too easily, Karrass tells us the target won't feel as good about winning the concession. From a negotiation standpoint, the person using the technique wants to do this at the end to close the deal so the target feels as if they have a hard-earned victory.

3.6.6 Commitment and consistency

These tend to go together in the sense that people want to appear to be consistent and to meet their commitments in order to be taken seriously.

3.6.6.1 Commitments are honored

If you can generate a promise of some sort, there will be a strong desire to fulfill it, no matter how much effort it takes or under what circumstances the promise was given. Fraudsters don't have this commitment honor and this is one of the main reasons they are able to take advantage of those who will fulfill their part of the bargains made. The target expects that the fraudster will fulfill their part of the bargain because the target has fulfilled their part of the bargain.

3.6.6.2 Consistency is highly valued

Once you commit, your interpretation of everything tends to support that committed view. Once you decide, automaticity leads to a desire not to rethink it and the commitment becomes one that is more likely to be retained as you see the world through it.

3.6.6.3 Small commitments lead to big ones

Self-image is raised through making and keeping commitments. As a result, larger and larger commitments are made over time. Think of all the frauds described earlier that take advantage of increasing trust with increasing demonstrations of keeping commitments.

3.6.6.4 Active commitments are better than passive ones

Commitments where you do something are far more effective at gaining subsequent compliance than passive promises. Saying yes to a telephone solicitation is less likely to produce an action than dialing into a public television donation line and promising a donation. That is because one is more active than the other. Fraudsters tend to induce action to get stronger commitments.

3.6.6.5 Public image leads to self image

Written statements are given more credence than oral ones both by author and reader. Public commitments are more often kept than private ones, so a public declaration of going on a diet or getting married is important to the success of these ventures.

3.6.6.6 Increased compliance with investment

Invested time and effort (sunk costs) increase commitment. The more pain involved the more it increases the commitment level. For example it has been shown that fraternities and sororities that haze more tend to have more loyalty from life-long members. You might say "more pain more gain". Less external return forces more internalization of value, and ownership and commitment follow. Low-balling works this way. You get a commitment, create other supports for the decision, then remove the original motivation, and the commitment remains.

3.6.6.7 Consistency causes decisions

Even when remaining consistent seems foolish, people will choose new reasons to stay with a decision because to do otherwise would cause them to have to admit they were wrong and rethink their previous commitments. Fraudsters often get a small commitment and then use compliance tactics as leverage to keep the target committed.

3.6.7 Social proof

Social proof is the replacement of proof that would normally be required with trust in those around you as adequate proof.

3.6.7.1 We interpret based on how others interpret

Laugh tracks work even if we know they are in use. Seeded collection boxes cause increased donations. Popularity is taken as goodness, even if the popular person is known to be wrong about what they are saying. In frauds, social proof is used all the time by the creation of a shill or multiple shills to create the social environment that induces desired behaviors. Politicians and propagandists use this all the time to try to suppress opposing views. They create the appearance that something is common even when it is unusual in order to make it socially acceptable.

3.6.7.2 Social proof replaces hard proof in uncertainty

Fear is reduced by watching others like you not fear. In some cases fraudsters will create uncertainty and generate social proof. Social proof works better when the people you are trusting for your proof seem to be like you are. A great example of this is fear of terrorism which creates uncertainty, and the seeming bravado of politicians then creates the social proof that the leader knows how to solve the problem and thus can make you safe.

3.6.8 Liking

People tend to react differently based on what they like and dislike.

3.6.8.1 We like saying 'yes' to people we like

People are twice as likely to say "yes" to people they like. Referrals from friends increase the likelihood of success in sales. MCI's "friends and family" promotion is 90% effective because it "does a friend a favor" to switch. Most fraudsters seek to create some sort of empathy with their target or take advantage of an existing friendship or relationship. George W. Bush is more likable than John Kerry, so it's easier to say “Yes” to Bush.

3.6.8.2 Physical attraction increases liking

People are more likely to like someone they are physically attracted to and likely to dislike someone they are not physically attracted to. Frauds that are up close and personal tend to exploit beauty when available. John Kennedy and his wife Jackie were far more physically attractive than Richard and Pat Nixon and this made them more “likable” even though Nixon clearly had a better understanding of foreign policy at the time.

3.6.8.3 Similarity breeds liking

Similar dress, color, background, behaviors, accents, lifestyle, interest, age, religion, politics, and names are all examples of how similarities increase liking and differences decrease liking, even when known to be falsehoods. Look at political processes where city slickers are wearing cowboy boots and going hunting. Southerners tend to vote for people with a southern accent and speech patterns. Of course California voters tend to vote for movie stars, which all Californians think they are like... OK, that's not really right, but it sounds like something you might say, so I used it.

3.6.8.4 Compliments increase liking

Even when compliments are known to be deceptions, people still like those who give them - unless they go "too far". Flattery will get you everywhere! How lovely you look when you are reading my book! Just imagine how lovely you will look reading my next one!

3.6.8.5 More contact increases liking

Familiarity improves liking unless the experience is unpleasant. So just being present increases the chances of being liked and provides the potential for increased interactions. Smile and don't talk much and you will probably be liked. Many fraudsters crash parties and meet people to become thought of as part of the group. They then get invitations and pretty soon integrate themselves into the group.

3.6.8.6 Groups working together bond

Common cause increases liking and friendship between group members and groups. This is a very common fraud technique in that the fraudster creates the situation in which the target and the fraudster end up seemingly aligned with each other and in a position of mutual trust. It's a partnership and you hold the money (or at least the bag that looks like it has the money).

3.6.8.7 Groups in competition breed enemies

Competition creates hostility and personal dislike. Fraudsters never want to be disliked, except in cases where they want to blow the victim off at the end of a fraud scheme. They can use falsified enemies to create common cause. For this they use shills.

3.6.8.8 Messages are attributed to messengers

When a message is unpleasant, the messenger is disliked, while good messages cause messengers to be liked. The attributes of the message are attributed to the messenger by association. In my security practice I find that this is a major killer. I seem to almost always deliver bad news when I assess security or suggest issues that have to be addressed. This is also one of the reasons that most fraudsters tend to present pleasant messages and one of the reasons that the most successful security “experts” always give glowing reports... even if the reports are completely wrong...

3.6.8.9 Association enhances liking or disliking

People are more receptive to compliance after a good meal. People associate to their nation, city, race, etc. and like it when the things they associate with succeed. This is abused by religious leaders, political leaders, and any number of others in positions of power who can use their bully pulpit to gain compliance.

3.6.8.10 People associate with self-image enhancements

If they like themselves, they choose to associate to things that are successful through the similarities to themselves. If they have a negative self-image they tend to associate with things that fail by seeking similarities with themselves. Fraudsters try to associate with their targets for enough time to gain the trust needed to perpetrate the fraud. They tell their targets how trustworthy the target is and that makes the target feel good about themselves and, by extension, about the fraudster. But you knew that all along, didn't you!

3.6.9 Scarcity

When there are long gas lines, the price is high, and people wait even longer for gas. Why is this?

3.6.9.1 Perceived scarcity increases perceived value

This is similar to Shannon's information theory in which less frequently used symbols have higher information content. Scarce quantity, time, or availability all make things more attractive and more precious. Fraudsters play this a lot. For example, when they join with aging rich people they say things like how precious the little time they have left together is. Why are diamonds so precious? Because an artificial scarcity was created by the DeBeers company in the 1900s and supported by political leaders from around the world who enhanced the scarcity and, in some cases, ended up with a lot of diamonds.

3.6.9.2 Loss is higher valued than gain

In trading a loss against an identical valued gain, the loss is more highly valued. "A bird in the hand is worth two in the bush" comes to mind here. Fraudsters use this when creating fear of a loss or when creating an opportunity with little apparent chance of a loss and enormous potential gains.

3.6.9.3 Desire to have what is restricted

This is especially effective against teenagers and young children, but also quite effective against people of other ages. It is more effective if more restrictive. Exclusivity yields a desire to have. Thus Havana cigars and Russian vodka are more highly prized. Children of certain ages are particularly susceptible to this when their parents don't give them something they want. If someone else, perhaps someone over the Internet, offers it to them in exchange for a meeting, the child will go to the meeting to get it.

3.6.9.4 Desire to have it "our way"

Even if "our way" is actually not our way, the perception of choice increases desirability. This is of course used by advertisers. Burger King anyone?

3.6.9.5 Exclusive information is more valued

Secrets, information that others do not have, restricted information, all seem to make the information more valuable. Exclusive information about a shortage has more effect on driving up perceived value than the shortage itself. Fraudsters use this a lot in response to natural disasters where they increase prices artificially. Of course some call this supply and demand.

3.6.9.6 Drops from abundance to scarcity increase value

More value is attributed to something if it is first possessed then lost. For example, revolutions are far more likely after some political gains followed by retrenchment. Fraudsters will take advantage of this when they can. Think in terms of gasoline. In the Carter administration, the increase in gas prices drove the US to long gas lines and there was fear driven by OPEC's reduction in supply. This drove up the market value of gasoline. And again this happened when hurricanes struck the US refining capacity in the Gulf States in 2005. The “price gouging” happened because the station owners knew that the scarcity of available gasoline meant that no matter what they charged, people would pay it to be able to drive out of the way of the next big storm.

3.7 Organizational deceptions

Charles Handy ("*Understanding Organizations*", Oxford University Press, NY, 1993.) discusses organizational structures and behaviors and the roles of power and influence within organizations. The National Research Council ("*Modeling Human and Organizational Behavior*", National Academy Press, Washington, DC, 1998.) discusses models of human and organizational behavior and how automation has been applied in this area.

Handy models organizations in terms of their structure and the effects of power and influence. Influence mechanisms are described in terms of who can apply them in what circumstances. Power is derived from physicality, resources, position (which yields information, access, and right to organize), expertise, personal charisma, and emotion. These result in influence through overt (force, exchange, rules and procedures, and persuasion), covert (ecology and magnetism), and bridging (threat of force) influences. Depending on the organizational structure and the relative positions of the participants, different aspects of power come into play and different techniques can be applied.

The NRC report includes scores of examples of modeling techniques and details of simulation implementations based on those models and their applicability to current and future needs.

Greene ("*The 48 Laws of Power*", Penguin Books, New York 1998.) describes the 48 laws of power and, along the way, demonstrates 48 methods that exert compliance forces in an organization. These can be traced to cognitive influences and mapped out using models like the ones Karrass and Cialdini have put forth, only applied in group settings.

3.8 MKULTRA: Government Mind Control

Closely related to the subject of deception is the work done by the CIA on the MKULTRA project. (For details see the on-line collection at http://all.net/journal/deception/MKULTRA/index.html). In June of 1977, a set of MKULTRA documents were discovered. They had escaped the efforts by the CIA to destroy all records of this project. The Senate Select Committee on Intelligence held a hearing on August 3, 1977 to question CIA officials on the newly-discovered documents, and that led to widespread public disclosure of the efforts of the United States to explore and exploit mind control.

The net effect of efforts to reveal information about this project was disclosure of information on the use of sonic waves, electroshock, and other similar methods for altering peoples' perception. Included in this are such items as:

- sound frequencies that make people fearful, sleepy, uncomfortable, or sexually aroused;
- results on hypnosis, truth drugs, psychic powers, and subliminal persuasion;
- LSD-related and other drug experiments on unwitting subjects; the CIA's "manual on trickery"; and so forth.

One 1955 MKULTRA document gives an indication of the size and range of the effort; the memo refers to the study of an assortment of mind-altering substances which would (and I quote):

- promote illogical thinking and impulsiveness to the point where the recipient would be discredited in public,
- increase the efficiency of mentation and perception,
- prevent or counteract the intoxicating effect of alcohol,
- promote the intoxicating effect of alcohol,
- produce the signs and symptoms of recognized diseases in a reversible way so that they may be used for malingering, etc.,
- render the indication of hypnosis easier or otherwise enhance its usefulness
- enhance the ability of individuals to withstand privation, torture and coercion during interrogation and so-called “brainwashing”,

- produce amnesia for events preceding and during their use,
- produce shock and confusion over extended periods of time and capable of surreptitious use,
- produce physical disablement such as paralysis of the legs, acute anemia, etc.,
- produce 'pure' euphoria with no subsequent let-down,
- alter personality structure in such a way that the tendency of the recipient to become dependent upon another person is enhanced,
- cause mental confusion of such a type that the individual under its influence will find it difficult to maintain a fabrication under questioning,
- lower the ambition and general working efficiency of men when administered in undetectable amounts, and
- promote weakness or distortion of the eyesight or hearing faculties, preferably without permanent effects.

A good summary of some of the pre-1990 results on psychological aspects of self-deception is provided in Heuer's CIA book on the psychology of intelligence analysis. ("*Psychology of Intelligence Analysis*", History Staff Center for the Study of Intelligence Central Intelligence Agency 1999.) Heuer goes one step further in trying to start assessing ways to counter deception, and concludes that intelligence analysts can make improvements in their presentation and analysis process. Several other papers on deception detection have been written and substantially summarized in Vrij's book on the subject. (*"Detecting Lies and Deceit*", Wiley, New York, NY, 2000.)

For readers who have doubts about these things, I do not urge you to go to the Web site, download the full details, and do your own experiments to see how these things can be exploited. Just imagine the implications if you could build a machine that aroused sexual urges in people with sounds played on a stereo. It could be the end of Viagra as we know it today! But seriously, don't play with such things. Like most deception methods, there is real potential for serious harm to people. You don't want to be like the fraudsters.

3.9 Teams that use deception

Most frauds and deceptions are undertaken by teams. While fraud teams tend to be quite small and, in some cases they outsource much of the work. Other teams are larger.

3.9.1 Singles, a risky game

Like drinking alone, committing frauds alone is a risky business. If you slip up, you go to jail. If the target is tougher than you, you can get beaten up. If they don't buy it, you have no support. In short, very few individual fraudsters are successful and they are always at greater risk when they are alone. For street frauds, the singles tend to be more or less beggars or low end pick pockets.

Many financial and Internet fraudsters work alone because they have the advantage of position. Financial frauds in organizations with limited controls are usually perpetrated by loners. They either accidentally come across a weakness or have fraud in mind from the start. They don't need help and to ask for it would risk getting caught. Internet scams allow the leverage of information technology, and for reasonably skilled attackers, it doesn't really take more than time and effort on their part. As a rule of thumb, these are individuals.

Most cases involving the leak of classified information also involve individuals acting alone, except of course that they leak the information to someone else.

3.9.2 Pairs, the most common team

Most fraudsters work in pairs. Pairs works well because you only have one other person to trust. Perhaps it is a spouse or lover, maybe just a good friend. The money doesn't have to be split too many ways, there is help if you need it, and there is a mix of skill sets available.

Most pick pockets have someone they can pass the wallet to after they do the pick, and most of the frauds involving convincing the target of something use a shill (a partner who appears not to be one) to authenticate some element as an "independent" third party.

Partners are often used in telephone frauds for cases where the target wants to talk to someone in authority, and in most of our penetration demonstrations we use a partner for authenticating one of our folks in case the other one is questioned by someone at the site. A partner is very useful for protecting the health and safety of a team member. In larger teams, partners often watch out for each other and protect each others' backs. Lookouts are also commonly used to spot potential problems, and partners are used to identify possible targets for the special skills of the other team member.

Intelligence operations, which we will discuss later, usually have partners, but they are also part of a far larger team. Police sting operations tend to have partners because police always work with partners. If you look through most of the person-to-person frauds listed earlier, you will find that they involve partners.

3.9.3 Groups of 3-7

In most penetration tests I lead there are groups of three to five, and sometimes as many as seven, involved in our operations. These numbers have proven manageable by one person and they combine the special expertise of the members to make the operations more effective. If you think back to Mission Impossible (the television series - not the movies) they use groups of this size for a similar apparent reason, and of course A-teams in the military are typically groups of five people.

Fraudsters also use teams of this size for certain types of operations. For store front schemes, this is about the normal size, and most complex frauds use similar counts.

As an example of a fraud scheme (penetration test in this case) that you need to have about this many people for, my group sometimes has problems getting into buildings when the defenses are really good. What we do is a relatively complicated and highly coordinated deception where we take a badge from an employee going to lunch, use it, and ultimately return it to them before they are done with their meal. I won't go into further details, but it takes a team with good communications to carry it off.

3.9.4 Big teams and gangs

Teams larger than about seven are really no longer teams. They are more like gangs. They tend to commit frauds like running phone rooms that do large volume calling scams or large-scale mail order frauds. Few in-person frauds involve large numbers of people because the necessary choreography is far too complex to expect to get right, the costs are so high, and the benefits per person rarely reach the levels of smaller group frauds. Large scale deceptions are used in military operations and similar venues, but this is beyond the scope of this book.

3.9.5 Intelligence operations

Intelligence operations can take a wide range of sizes, but they tend to have some things in common. They usually have different facets to them, and in combination, form what is commonly called "all source" intelligence.

3.9.5.1 All source intelligence

All source is what it says - all sources are considered. Generally, sources are given weights based on their history of trustworthiness and the information they provide is related back to them for analytical purposes. Intelligence from all available sources are then combined in analytical products that typically include not only the analysis, but also the basis for that analysis. The basis is, in essence, the attribution to source combined with reliability of the source and integrated with information from other sources that touch on the credibility of the result.

3.9.5.1.1 The basis for trust

As a rule of thumb, intelligence usually reports uncorroborated information only if their impact is potentially high and their source reasonably reliable. Rumor, innuendo, and similar information tends to be discounted while facts that can be proven and whose evidence is included tend to be elevated. Or at least that is what is supposed to happen. Sometimes intelligence goes awry and emphasizes rumor and unreliable sources and reduces the value of trusted sources. The result, regardless of the cause, is the sort of intelligence blunders seen throughout history.

3.9.5.1.2 External distant efforts

In order to do red teaming sorts of intelligence operations, a team of 2-5 people is usually used for distant efforts like searching public records, the Internet, libraries, making calls, and doing technical scans. While a single individual can do this process, there is a tendency to get better results sooner when several people are used. I tend to want groups of 5, usually with a few relatively inexperienced folks who will question everything, a few old hands with specialized expertise, and a team leader with strong intelligence experience and a history of winning. This is because people tend to have blinders. I usually act as an external reviewer because of the potential for group think. Most fraudsters use only one person for intelligence of this sort, while governments have larger sets of teams each specializing in one area and are supported by a lot of tool development and analysis databases.

3.9.5.1.3 Technical measures

Technical surveillance and technical capabilities are planted by intelligence operations in order to provide ongoing information and the ability to affect the opposition. In red teaming efforts, we rarely do this because (1) it is not necessary, (2) it verges on illegal unless there is explicit control and approval at every step by the client, and (3) it usually costs more, takes longer, and our efforts are not granted that kind of budget or time. While we do use technical tools like network scanners and plant surreptitious devices like wireless access points into networks, and we demonstrate the use of other similar devices, in red teaming efforts that we undertake it is not necessary to actually apply most of these tools. Once planted, we prove it to the sponsor and then remove it. For analysis purposes we can then determine what could reasonably be done from there and move on.

The CIA is famous for its amazing technical intelligence tools, like spy planes and satellites, planting surveillance devices in an under-ocean telecommunications cable used by the Soviet Union, computer surveillance, special electronics, small cameras, and so forth. The Soviet Union was also well known for bugging the American Embassy in Moscow and planting the "Thing" in a gift.

3.9.5.1.4 Human intelligence

Fraudsters use human intelligence almost exclusively. They often have a spotter that identifies the mark (target) and people who undertake these activities tend to gain excellent skills in determining who will be compliant and who to avoid. They can often spot police and investigators by their shoes or habits or the way they walk. They also use the "word on the street" to learn about what's going on through rumors, and they sometimes undertake simplistic intelligence operations like Internet searches or find their targets through the newspaper, as in funeral schemes. They might go to lonely hearts clubs for sweetheart scams and so forth. They are skilled hunters but only in the sense that they have a keen eye and practice telling the difference as a survival matter.

Police have intelligence capabilities and units and do undercover work to detect who is doing what. They do technical surveillance including wire taps and body wires in support of this intelligence effort, and they have databases ranging from local records systems to the NCIC and Interpol database systems. These include detailed records of individual criminals including finger prints, DNA patterns, detailed histories, and so forth. Police around the world do more human intelligence than any other organization.

In our Red teaming exercises we do human exploitation and limited human intelligence efforts, and it almost always pays off. Whether it is perception management against employees from over the telephone, meeting folks at local bars, or using information we have gathered in other ways to leverage perceived similarities, these techniques work. But in red teaming there is rarely enough time to build up a real relationship and we certainly don't want to create love affairs with employees of our clients in order to prove that we can get them to steal from the client. Human intelligence at the level of a national intelligence agency is the trickiest one to accomplish and this will be discussed at length later under the topic of elicitation. Suffice it to say that it takes many years of effort for national intelligence operations to even get properly started.

3.9.5.1.5 Military sources

All military organizations include intelligence operations. There are usually intelligence officers at every level of command. In the US military, the intelligence capabilities are stunning and both a strategic and tactical advantage. Through a complex global system, detailed information from all levels are fed into a global intelligence system that gives near-real-time information on the battlefield. The fog of war is nearly gone from some environments. The military also has operatives that feed this scheme and researchers that do other elements of all source intelligence.

3.10 How far can you move people?

The idea of most fraud schemes is to get the target(s) to change their normal behavior into the behavior desired by the fraudster. The fraudster applies techniques that move the target over time in the desired direction.

3.10.1 Further faster is harder and riskier

Problems tend to arise when the desired goal is far afield from the normal behavior patterns of the target(s). The reason is that this requires more simulation and concealment and more substantial changes in expectations. This in turn increases the odds of being detected and associated with the true cause, with a resultant increased potential for failure of the deception.

3.10.2 Hopes and dreams support rapid change

On the other hand, meeting or exceeding the expectations and exploiting the hopes and dreams of targets makes the fraud highly likely to succeed. Ego and greed play an important role in the success of frauds against people.

3.10.3 It's hard to fool an honest man?

No it isn't. This is just a fallacy. In fact, honest people tend to think that others around them are also honest and they often find it hard to believe that they are being lied to. Honest people are very commonly the targets of frauds, and sadly, older people are the most picked on group because they tend to be more easily deceived and have enough money to make it worthwhile.

3.11 Some common fraudster characteristics

People who commit frauds typically have certain things in common. Of course there are exceptions to every rule, but for the most part these things are true.

3.11.1 Full-time fraudsters

People that commit frauds for a living are typically just a bit different from the opportunistic fraudsters.

3.11.1.1 They don't care but look like they do

Despite their appearance as kind, thoughtful, and friendly people, fraudsters do not care about their targets. The term sociopath was once common for this behavior, but that has fallen into disuse In many cases fraudsters are not at the extreme end of the spectrum. They may justify their actions to themselves by saying things like "I only ever stole from someone who was trying to steal from me" or "I never took money from anyone, they gave it to me".

3.11.1.2 They give no quarter

Those who have fallen for phony prize frauds or other similar frauds are called again for other frauds. In essence, once you get nailed, fraudsters mark you as easy prey and come after you again and again, sometimes even selling information about you to other fraudsters. Of course there is also the fraudster defrauding aspect of these name lists, but that's a different story.

3.11.1.3 They have targets for what to take

Typically, a fraudster that has stolen most of your money will want to come back and get the rest. But different sorts of frauds involve different amounts that can be taken. Short cons and one-shot deals seek to get a fixed amount of money now - everything you have in your pocket so to speak. Longer frauds seek to take everything you have, including your home and family.

3.11.1.4 They move around a lot

Most fraudsters move from place to place. They stay only a few weeks at the same location, depending on the time before they are likely to get caught. This is part of a bigger theme. They have pretty substantial time limits on their activities so they end up having to rush things at times, putting time pressure on their targets.

3.11.1.5 They have no shame

People that perpetrate most frauds are just liars and thieves that take advantage of other people by exploiting their weaknesses. They prey on the weak of society and steal from the poor and disabled. They steal from babies, hurt old defenseless people, misuse the trust people put in other people, and generally degrade the overall level of civility and niceness in society.

3.11.2 Opportunistic fraudsters

Opportunistic fraudsters are said to constitute about a third of all employees. They usually take little things here and there, but unlike most employees, they may go to extremes. They don't try to think up new frauds all the time, but rather they encounter system quirks and once they accidentally or "legitimately" get around the system, they decide to do the same thing for advantage or "compensation".

3.11.2.1 They are mad at their employer

Most employees who take substantial amounts opportunistically from their employer are disgruntled. They take it out through the frauds as “compensation” which allows them to justify their behavior to themselves. They start out small and accumulate more over time, sometimes adding up to a substantial amount.

3.11.2.2 They happen across a flaw

Many opportunistic frauds happen when a way of doing things at the business happen to lead to a way to take more than the employee should. Sometimes it is done as a completely legitimate bypass. For example, you go on travel and take a taxi, but you lose the receipt for that taxi ride. But since you have several other similar receipts, you copy one of them on your copier, change the details to be whatever you actually paid for the taxi ride, and submit the forged receipt for reimbursement. This is not a fraud, of course, it's just not "the original" receipt.

3.11.2.3 They expand on the idea

Now that the employee understands this and has done it once, the temptation arises to use it again, but perhaps somewhat less legitimately. The next time, it might be a meal where they have a receipt but since other folks they know are on per diem, they feel like they should get per diem. After all, they could have had a $20

lunch instead of a $5 lunch, and their co-worker did. So it''s only fair that if I choose to eat less the company shouldn't punish me. In fact, I'll only charge them $15, so I am saving them money! As the logic twists, they are doing the company a favor.

3.11.2.4 It gets normalized then out of control

I did it last week, so I should be able to do it this week. That's the logic as the taking by lying starts to grow. Why not charge for a client lunch even though I ate alone? How can they tell what I had to eat at the airport? They didn't compensate for lunch last week because I forgot to charge them, so I'll charge them double every day this week. I think I may be fired soon because they are really pressuring me for more sales, so I may as well get mine while the getting is good.

3.11.3 Desperation fraudsters

A completely different sort of fraudster grows out of desperate times. People who have little or no money and are living in squalor tend to have dramatically reduced standards for what they are willing to do to survive. Whether it is stealing bread when you are hungry or money when you are destitute, desperation drives people. Normally honest people about to lose their home or the health of a family member get desperate and take what they can from where they can get it. Even people that appear to be wealthy may in fact be desperate for money, in many cases because they cannot afford to support their lifestyle.

3.11.4 Never enough fraudsters

It is hard for most people to believe that an executive making millions of dollars per year would try to steal a few million extra dollars by perpetrating a fraud. But they do.

3.11.4.1 Keeping up with the Joneses

It sometimes starts with the competitive nature of people. Keeping up with the other wealthy business executives means big houses, private planes, luxury vacations, and custom tailored suits. Each seeks to outdo the other.

3.11.4.2 It's for their own good

Life is short, and as long as I am in the position of power, I deserve all the perks that come with it. If the board of directors won't approve a private jet, I will arrange to get one through a trick and then claim to be using my own jet instead of theirs. After all, I need a private jet to save time and inconvenience that make the difference between closing the next big deal and missing it.

3.11.4.3 That's how I got here

When I was a junior executive I used to take first class all the time, even though the company policy was to take tourist class. I was always fresher when we arrived and better able to make and close the deals. I need the fancy car to make myself appear successful. What executive doesn't have a chauffeur? I wouldn't be CEO of this company if I didn't know that you need to invest in order to prosper. They knew what I was doing, so they must tacitly approve. After all, I got most of the board of directors their appointments anyway.

3.11.4.4 I deserve it

They only pay me $12 million a year, but I grew the business from $500M to $600M last year alone. If they can't see that I deserve a raise, I'll take it out in perks.

3.11.4.5 They dictate behavior by rewards

They pay me to get the stock price up, and that's exactly what I'm doing by cooking the books. My bonuses are driven by the bottom line, and if they wanted me to make the company stronger for the long run, they would give me a bonus for that instead.

3.11.4.6 Everybody does it

Every executive worth his salt knows that you don't evaluate inventory based on what you think it might be worth. You maximize shareholder value by claiming all inventory has its maximum value. That's how you keep the share price up and that's how the shareholders make money when they sell their stocks. Of course I know that the company will be able to sustain this growth for 2 or three quarters before things drop back down. That's why I'm selling my stock now. As long as I announce sale of my stock in advance, I've met the legal requirement. It's a blind trust, so what if my best friend runs it and we chat about other things every day?

3.11.4.7 They haven't gotten me yet

I've been doing it for the last 5 years, and I'm still here. Sure they are investigating, but they will never catch me. Just use the offshore accounts and buy in smaller amounts - spread it out more. Better cool off for a while, we'll claim it's a cost cutting measure and then start doing it again next quarter after I make my numbers.

3.11.4.8 Look mom, I'm on top of the world!

Jimmy Cagney in "*White Heat*" is the reference here. If you haven't seen the movie you should get a copy. No, I did not get a fee for the endorsement.

3.11.5 Professional intelligence operatives

Professional intelligence operatives have none of these sorts of characteristics. The most effective ones are just everyday people with everyday jobs that take them to the places they need to be to do their intelligence activities. They look like you and I, act like you and I, and fit in without making a splash or standing out in a crowd. Their survival depends on not being dashing or flashy or overly noticeable.

3.12 Where to learn more

One of the best books on historical frauds is called "*Extraordinary Popular Delusions and the Madness of Crowds*" by Charles Mackay (Richard Bently publisher, 1841). This book covers many large-scale historic deceptions from long ago in wonderful detail and represents a hallmark in the field. I was led to it in the late 1990s when the Internet bubble was underway and many folks seemed to know it. But it turns out that during bubbles, the goal is to know when to walk away, and not to walk away too soon.

For those interested in military deception, the best book from my view is called "*Military Intelligence Blunders*" which was written by Colonel John Hughes-Wilson (Carol & Graf, NY, 1999). This book does a really find job of describing the sorts of blunders made by leaders in using military intelligence operations and details many historical blunders as examples. The lessons pointed out in this book seem to be supported by subsequent events as well and anyone who is concerned about this issue should most certainly read this book. Several other books are used in schools run by the US government and elsewhere for teaching fraud investigators how to ply their trades. If you are interested, you should try to find books on the subject.

The FBI also has a Web site on recent frauds. Just go to your search engine and look for "FBI Frauds". They usually list a top-five or top-ten set of frauds that they see most frequently.

4 Elicitation and intelligence operations

The real professionals in the frauds game are the intelligence operators who take advantage of human weakness for a living. When they describe these issues, they talk about exploiting specific sorts of human weaknesses.

4.1 Elicitation strategies and tactics

Elicitation is not just something that happens all on its own. It is a systematic approach that mixes specific skills, talents, and experience with well-defined objectives applied against sources using methods that allow strategies and tactics to be successfully applied. When you hear a government discussion about the intelligence community that talks about how critical it is to protect sources and methods, this is what they are talking about.

4.1.1 Sources and methods

Sources are the people or things that have the information the intelligence operatives seek or who can get that information or make those things available either directly or indirectly. Examples of sources include but certainly are not limited to:

- Individuals
- Surreptitious surveillance technologies
- Trojan horses in computer hardware or software
- Satellites, submarines, or other technical wonders

The old saying in the intelligence business goes: "I could tell you but then I would have to kill you." And they sometimes mean it. So I will not try to go into elaborate details on this subject, and of course there are plenty of books that cover it. One of the best is endorsed by both a former head of the KGB (Oleg Kalugin) and a former head of the CIA (William Casey) - talk about credentials! It is called: "The Ultimate Spy Book" by Keith Melton, DK Publishers, 1996.

Methods include the technical methods, but they also include the operational methods - the things people do - how they get to the sources - things like that. For example, for some time the CIA was using business people (according to the press - the CIA essentially never talks about such things so you never know) who travel internationally as intelligence operatives. Assume it is true.

If they have business people who work for foreign companies getting information by making friends with executives and gaining consulting contracts through which they gain the capacity to plant special purpose intelligence gathering hardware in client facilities, that would be a method. Obviously this method has to be protected or else whatever planted assets are available would be searched out and removed or exploited to feed false information. If you don't know the method you are left searching everything for anything all the time, and of course that makes your country fall apart from the excessive spending (think about the former Soviet Union).

As another example, in the case of "outed" CIA covert operative Valerie Plame, the CIA was using people who did whatever it was that she did, as intelligence operatives. Of course she wasn't the only person doing what she did to get intelligence from folks in other countries, so when the world found out that she was an intelligence operative, all of the other similar operatives immediately become suspects along with the other similar people who are not operatives. And everyone they ever met with or talked to comes under suspicion. The front company she “works” for and all similar companies and all of their employees and contacts come under scrutiny. Her life is examined in detail to reveal possible methods. Of course anybody in an oppressive regime that ever met in private with Ms. Plame is likely to get tortured and shot. So much for our sources. The intelligence assets are lost so we can no longer gain the intelligence we were getting from them.

All of this is a long winded way of (1) explaining this to the Republicans who would be explaining it to the Democrats if the Democrats had outed Ms. Plame and (2) pointing out that I won't be pointing out any specific sources or methods except those that are already published. Not that I would know of them anyway, but if I did I certainly wouldn't tell you in a book. You would have to elicit them from me.

4.1.2 Tactics and strategies

I will, however, tell you about strategies and tactics. These elicitation tactics and strategies allow the manipulator to bypass the target's normal rational and critical decision processes by applying the notions of deception described earlier to specific effect in the even bigger confidence game of human intelligence gathering.

But first a word from the U.S. government...

4.1.3 According to the Department of Energy

Here is what the US Department of Energy says about elicitation on one of their publicly reachable (at one time) Web sites. It is also on the Web at:

http://rf-web.tamu.edu/security/secguide/T3method/Elicit.htm

and you might also want to look at:

http://www.ch.doe.gov/offices/OCI/Elicitation/

In the spy trade, elicitation is the term applied to subtle extraction of information during an apparently normal and innocent conversation. Most intelligence operatives are well trained to take advantage of professional or social opportunities to interact with persons who have access to classified or other protected information.

Conducted by a skillful intelligence collector, elicitation appears to be normal social or professional conversation and can occur anywhere – in a restaurant, at a conference, or during a visit to one's home. But it is conversation with a purpose, to collect information about your work or to collect assessment information about you or your colleagues.

Elicitation may involve a cover story or pretext to explain why certain questions are being asked. Some elicitation efforts can be pretty aggressive, imaginative, or involve extensive planning. For example: A professor from a south Asian country was teaching a night class in business administration at a Maryland university. In one assignment, her students were assigned a term paper on the company where they worked. One student reported to the FBI that

her paper was returned by the professor three times. On each occasion the professor asked for more details on the company. The student became concerned when the directed expansion of the assignment began to involve sensitive, possibly proprietary information. (Rusty Capps, "The Spy Who Came to Work," Security Management, February 1997.)

For the foreign intelligence operative in the United States, one attraction of elicitation as an intelligence-collection technique is that it is a very low risk activity. It is hard for the target to recognize as an intelligence collection technique and easy to deny any intentional wrongdoing. It is just a pleasant conversation among colleagues or friends.

Another attraction is that it often works. Through elicitation, intelligence collectors may confirm or expand their knowledge of a sensitive program or may gain clearer insight into a person's potential susceptibility to recruitment.

As an intelligence technique, elicitation exploits several fundamental aspects of human nature:

- *Most of us want to be polite and helpful, so we answer questions even from relative strangers.*
- *We want to appear well-informed about our professional specialty, so we may be tempted to say more than we should.*
- *We want to be appreciated, and to feel that we are doing something important and useful. As a result, we often talk more expansively in response to praise about the value or importance of our work.*
- *As open and honest people, we are often reluctant to withhold information, lie, or be suspicious of others' motives.*

Testing willingness to talk about matters of intelligence interest is one step on the road to recruitment discussed in How Do I Know When I'm Being Targeted and Assessed? If you provide useful information once, you may be considered a "developmental

contact." If you do so regularly, you may be classified as a "trusted source."

You should feel free to expand your professional and personal horizons by meeting with foreign colleagues, as long as you keep in mind that not everyone you meet has the best intentions. Follow these rules when talking with foreign colleagues:

- *Never talk about your personal problems, or about the personal problems or weaknesses of an American colleague. Such information may be exactly what the other side is looking for.*
- *If the conversation is moving into a sensitive area, change the subject or simply ignore any improper question. You are not obliged to tell anyone any information they are not authorized to know.*
- *To discourage someone who seems to be too pushy about discussing sensitive information or arranging a private meeting with you, state that you would have to clear this with your security office. That is the last thing an intelligence operative wants to hear. It usually causes him/her to back off immediately, as no intelligence operative wants the FBI or CIA to become aware of their contact with you.*

I guess it is pretty clear that the US government has deep concerns about elicitation to gather classified information, and rightly so. But the same elicitation tactics are used by fraudsters all the time, and that's why it is so interesting to study those strategies and tactics here.

4.1.4 Does this sound like a reporter to you?

Reporters are generally pretty good at elicitation. The same tactics used by intelligence agents are used by reporters, so it should not be surprising that they manage to get access to classified information and publish it. But you would also think that the counter-elicitation tactics of the US government augmented by the fact that the reporters are known to be reporters would reduce the level to which the tactics work. Apparently not.

4.2 Qualities of the effective elicitor

Certain people are better at certain things. So how do you tell who will likely be good at elicitation? That's easy. You make a checklist. And here is an example of one such checklist.

4.2.1 A gift for making people feel at ease

Some people just have a way of getting along with others, and other people don't. In my life, I have found some number of people that I just get along with, for whatever reason. Most people have. But that doesn't make me or you good at this. While you can probably develop this skill to make it better, people with the gift just have it, and I don't think it can be built.

4.2.2 Common sense and good judgment

I have a saying about this. Common sense is not that common. Judgment can be taught to some extent, but most people just have a way of screwing up every now and then. In an intelligence operative doing elicitation, this can get people killed, including the operative. It is particularly important to be able to recognize vulnerabilities effectively and not make bad judgments about these because these are tightly linked to the risky steps in elicitation.

4.2.3 Feeling for the subtle aspects of a relationship

I sometimes have this, but not usually. People who are good at this spend their time and effort thinking about their relationships. I spend my time trying to get what I do right and trying to fix things I think need to be fixed. That means that I am a better target for elicitation than practitioner. And yet, for small periods of time on assessments, I can almost always get these things to work. That's fine for assessment teams, but no good for a professional elicitor.

4.2.4 Good listener

Oh well... disqualified again. I am a better talker than listener - as most people are. But we all know good listeners and they are usually the folks we end up talking to. Which is why they are so useful in elicitation.

4.2.5 Quick and flexible mind

I like to call this "smart". One of my old managers used to talk about people who are quick as having high mental processing speed. They can think quickly on their feet and stay alert when bored nearly to tears.

4.2.6 Patience

Now we are getting tough. You have to be smart and quick and yet patient too. I get frustrated after only a few years of being blocked at every turn. But many intelligence operatives work on a case for five years or more before making significant progress, and in some cases, relationships are worked over decades before they really begin to bear fruit.

4.2.7 Fluency in the target's language

You have to be able to talk the talk and do it well or there is no hope of being able to build the sort of rapport you need for this business. Of course this fluency can either be cultural, as in knowing French and French culture, or professional, like being a metallurgist when attending metallurgy conferences.

4.2.8 Knowing when resistance is blocking progress

Some of us just blunder along not knowing when to go forward and when to back off. My wife will likely tell you (if she will talk to you at all about such things) that I just don't know when to back down. It's true. I go too far too fast and blunder into things that get me into trouble all of the time. And on the Internet I am more often than I should be, a "flamer". Yes - I push the "send" button when I should cool off, reread what I am sending, and cancel the request. But good elicitation experts don't have this flaw.

4.3 Effective conversational gambits

Conversational gambits are the little tricks that a person can use in a conversation to cause their target to reveal information. The skilled elicitor will adapt these to the target as needed. In fact, nearly 77% of all elicitation efforts apply 3 or more of these techniques in order to exploit known weaknesses in their targets. Which brings me to...

4.3.1 False facts

The information sought is stated as fact in an effort to get the target to confirm or correct it. In some cases the elicitor will introduce slightly erroneous information to get it corrected and/or may attribute it to someone else, perhaps a competitor of the target. This is done in hopes of eliciting a correction or elaboration by the target.

4.3.2 Disagreements to keep the ball rolling

The elicitor partially disagrees with the target to keep the ball rolling and get them to clarify or respond to the challenge. Either total agreement or total disagreement tend to end the conversation or disrupt the flow, both of which the elicitor wants to avoid.

4.3.3 Flattery

As my brother used to say, “flattery will get you everywhere.” The target may be approached as an authority on a subject and asked for advice. A remark may be made on the paucity of information available on a particular topic. Since the target is known to be so knowledgeable about it, the elicitor expresses the hope that they could share their expertise. If the target is of lower professional status, they may like being treated as an equal and try to earn the status by demonstrating their expertise. Deft flattery may be directed against a target, their spouse, profession, or institution.

4.3.4 Handouts

Sometimes you have to give to get. Elicitors may provide some piece of information that the target doesn't know or that appears to be sensitive or classified as bait for future requests. This uses the principle of reciprocity to elicit returns in kind. The reciprocity may be in the future, so don't think that one meeting is all it takes. It also gives the appearance that the elicitor has access to classified information, which then authenticates them as a trusted recipient.

4.3.5 Oblique references

The elicitor may make an oblique reference to something known to the target hoping that the target will fill in missing information. It implies that the elicitor knows all about the subject already.

4.3.6 Negative approach

In this approach, the knowledge of the target is called into question to cause them to prove that they are experts by demonstrating their knowledge. "No one here could possibly know anything about how the “Thing” really worked." The target then shows off by telling a story about it to prove they know of the resort.

4.3.7 Incredulous approach

The elicitor may state that some fact could not possibly be true or that a device to do this or that could not exist because it is impossible: "Where did you get that piece of misinformation." or perhaps that the target could not know it: "Who told you that... you can't possibly know about that." The hope is that the target's ego will be challenged and vindicated by proving that they know what they mean by providing further details.

4.3.8 Privileged colleague

The elicitor may present themselves as a colleague that can be trusted in order to gain confidence of the target. "Hi Jim, nice to meet you. I'm just in from the Omaha office for the week. Gee, did you hear about the latest rumor from the R&D department? They claimed to ...".

4.3.9 Misdirect and retreat

In this gambit, the elicitor focuses on a sensitive topic that they care little or nothing about, providing wrong or false information which the target rebuffs. The elicitor then retreats to his true topic of interest, hoping that the target will feel apologetic for the rebuff and be willing to discuss this matter in lieu of the original topic.

4.3.10 Discussion of others

Discussion of others in the field and their views will often provoke a person to either associate or disassociate with the referenced others, perhaps with stories of specific disagreements or collaborative works.

4.3.11 Alcohol and women

These old standbys are still frequently used as aids to collecting information. They are especially good if the subject is lonely, tired or has been under a strenuous schedule.

4.3.12 Use of the gambits

The good elicitor detects resistance to their attempts and tries other tactics, knows when to back off, and replaces themselves with an alternative when tactics start to fail, in hopes that someone else will do a better job of it. Very similar tactics are used in interviews by police and others in order to get perpetrators to reveal the truth. In these cases resistance is readily detected by answers that are evasive or overly general. These gambits are among many methods used to influence others, however, they are very tactical in the sense that they work on the time frame of seconds within conversational contexts.

4.4 Exploitable traits

There are certain human traits that make influence tactics effective. The ones most commonly exploited in elicitation are identified here.

4.4.1 Tendency to talk when they are listened to

Most people want to be listened to and many people feel as if they are not listened to in the normal course of their work or lives. When someone is willing to listen, these people - most people - are willing to talk. They tend to like people that listen to them. In fact, silence is often intolerable in a conversation and will cause people to either leave, talk, or express deep frustration.

4.4.2 Desire to correct mistakes or inconsistencies

When people know something is wrong in what another person says, they have a tendency to want to correct it. This is especially true in men, scientists, engineers, and young people. Many people have an argumentative view of the world at times and this view is exaggerated by frustration in many cases.

4.4.3 Need to gossip

You know, of course, that lots of folks love to gossip. Why just the other day, I heard that... oops, better get a grip on myself.

4.4.4 Curiosity

It may have killed the cat, and there are certainly a lot of curious people. People that want to know things tend to ask a lot of questions about the things they are interested in. The questions themselves are often revealing. For example, someone in a bank

that asks over the Internet about some specific configuration issue associated with a particular kind of computer is revealing that the bank has that kind of computer with that kind of configuration problem. Scientists and politicians often ask questions about the things they are concerned with, and the questions they ask indicate what they are afraid of or interested in. If I bring up five different things in a conversation and there is little curiosity about three of the five, a light hit on one, and intense interest in the other, it may tell me a lot about the program the individual is working in.

4.4.5 Inability to keep secrets

People are often just no good at keeping secrets, even when they know they are secrets. For one reason or another, they end up telling someone something. In fact, there is somehow a deep seated desire to share what you know with other people. And if it is easy to do because there is no perceived threat present, or because it happens to come up in casual conversation, why not?

4.4.6 Need for recognition or feeling of importance

I have an old friend who I spent some time with just a few weeks ago, who just had to tell me about his breakthrough research. I think he was just plain frustrated by the fact that nobody appreciated the thousands of things he had to do in order to come up with the result he eventually got that was a really wonderful result. It was one of those things that he hoped I would appreciate and it is likely that this is because he doesn't feel appreciated at that sort of technical level from others he encounters. If I was trying to elicit from him, I likely could have turned it into something bigger, but I was trying not to think about work at the time, so I told him I thought it was cool and let it pass without further elicitation. If people volunteer information like this when they are not being professionally elicited, imagine how much you could get if you wanted to go after it.

4.4.7 Underestimating importance of their information

I know that things like “which of five areas brings out curiosity” or “the correction of a minor mistake” may seem trivial to you, and they often seem trivial to targets of elicitation. But the intelligence game is one of taking small bits of information and assembling

them into a mosaic. Intelligence operatives rarely encounter a James Bond moment when the girl working for the Chinese classified nuclear weapons program happens to fall in love with the secret agent and also happens to know exactly the critical secret required to save the world. I will provide more on the mosaic problem later.

4.4.8 Habits that a manipulator can exploit

People have needs and wants and habits associated with getting them. These habits can often be exploited. For example, the Mazlov hierarchy includes survival needs like air, water, food, and shelter; and higher level needs like safety, health, and comfort. People who want more money can be brought into compliance by offers of better deals, gifts of fine wines, and other similar items. People looking for comfort can be given gifts like new jackets and so forth. And of course these can be loaned and taken back as subtle rewards and punishments.

There are also habits that people get into like having their morning coffee at the same place every day and always putting their keys on top of their desk when they go out to lunch. These habits create predictability that can be exploited for everything from breaking and entering to figuring out how to have a new agent meet with the target and what sorts of things to talk about. If a target goes to the same bar every Thursday night trying to pick up members of the opposite sex, one of those nights, the right elicitor can show up with the proper attire and attitude and go a long way to creating a workable elicitation relationship.

4.4.9 Emotional vulnerabilities

People that are away from home for long periods, that are having problems with relationships, that have recently lost a loved one, or that have other momentary emotional difficulties are often more susceptible than those who are in a stable situation among friends and family at home.

The Russians are well known for exploiting the loneliness of US government workers who are in Russia for one reason or another for extended periods of time. Their efforts include professional mistresses who latch onto Americans and turn them into intelligence assets. In some cases they have combined this with legal system methods, like one case where a worker ended up having sex with a teenager, was then arrested, and was told, in essence, that it was jail for 20 years in a gulag or revelation of classified information.

4.4.10 Tendency to "talk shop" with colleagues

In a friendly atmosphere, like a party at a professional conference, people talk about their work. The skillful elicitation expert can leverage these conversations to gather small tidbits of information on their shopping list of things they want to know and to create new relationships for further exploitation in the future.

4.4.11 Susceptibility of personality in situation

People are more or less subject to influences depending on their situation and personality. I was once in Taiwan for a free full-day short course I was supposed to give for the Institute of Electrical and Electronics Engineers (IEEE) about computer viruses. Of course this was for no fee, so I had to find a way to pay for the trip to Taiwan. Along comes a company that I knew some folks from and I ask them if they will pay a small fee in exchange for me giving a course to their folks and their clients. That allowed the trip to cover my expenses and pay me a little bit for my time.

When I arrived, I gave the course for the company and then proceeded to the IEEE conference. But the conference organizers were in a huff about me doing this other work because they had paid a part of my airfare and thought it was inappropriate for them to pay airfare when I did commercial work. I thought this was outrageous that every other attendee was being paid for their time by their employer and, as an independent consultant, I was the only one not being paid, when I was teaching the course. For them to tell me that I can't make a living so I can give them a free talk rather upset me. But the money is not the issue here. The issue is

that they put a big squeeze on me by threatening not to reimburse my airfare, cancel my talk, and so forth. It caused me a good deal of emotional strain because I was in a country across the world, knew nobody there, and I was staying in a dormitory where there were no phones or other methods of communication, and nobody spoke English. I was cut off from everything and being left to wait for an arbitrary decision by people who were being unfriendly toward me. And of course I was jet lagged and exhausted. I figure that would have been the perfect time to elicit me. Nobody did.

4.5 Life sources of human weakness

Not all of the exploitable traits are always available. In fact, there are common life events that cause people to become susceptible to elicitation tactics (and other frauds). They tend to correspond to the things in life that bring emotions to the fore at higher levels than usual. They are the stressors of life.

4.5.1 Youth and exploration

Small children and others who have not yet experienced the level of deception that happens to most of us every day are naive to the point of simply going along with almost anything that sounds like a good story. They will tell anybody anything they know. Try becoming a babysitter for the target and you will likely learn all about the weaknesses of the individuals and eventually become very close to the family members. This was used on a few occasions in World War 2 when babysitters for German General Staff members were the targets of Allied intelligence efforts. It is likely still used by all sides when available.

The transition to and from teenager is also fraught with emotional difficulties as children find their way to separate from their parents and become lonely and sway back and forth between children and adults. These times bring stress on both the child and their parents and lead to a wide range of complications that can be exploited in any number of ways. Teenagers in trouble create parents who need money. Fighting at home creates a desire for understanding from other places. Sexuality emerging brings a wide variety of challenges to parents that may be met in a wide variety of ways.

4.5.2 Transitions to and within work

Most new employees are excited about their new jobs, although there are certainly exceptions. But over time a significant number of these employees become disenchanted for a time for one reason or another. They become disgruntled and their behaviors and susceptibility to elicitation change. When an employee is looking for a new job and still has their old one, it is a sign of being disgruntled, a good elicitor will take advantage. But it is not just problems that create opportunities.

In many cases, elicitation takes place when people get raises or promotions. The joy of the moment when someone gets promoted is often shared with friends and stories are told about how the advancement happened or other work-related matters. Raises often generate buying a round at the local pub or having a celebration with friends and family. Remember that an elicitor is in the job of being friends to the people that have the information or influence they want to exploit.

4.5.3 Marriage and divorce

Weddings, if you can get invited, are wonderful opportunities to learn all about people and their families. Wives tell on husbands and husbands tell on wives. Family members tell stories about all sorts of things. People get drunk and their guard is usually lowered. And there are higher costs than normal. All of these are opportunities to the elicitation expert. They represent chances to corrupt the system and the people in it.

4.5.4 Middle age

When you get to a certain age you start to realize that you are really only driving toward death. So what do you do? That's easy - get a sports car, learn to scuba dive, jump out of an airplane (with a parachute I hope), have an affair, or get plastic surgery. These are just some of the things people do when they find out they are getting older and that they are running out of time. They want to live life now and do wild things that remind them of their youth. They want to shed responsibilities, feel free again, feel attractive and gay and full of energy. And of course, all of these are things

that provide opportunities to the elicitor. Want a sports car? Borrow mine for a while - it's little enough to pay for the information you gave me last week - I made a fortune in the markets from it. Want to use my apartment for having an affair? No problem - here's the key. They usually don't tell you about the cameras until after they start to squeeze you for more information than you want to give.

4.5.5 Getting old and retiring

Getting old is better for fraudsters than for elicitors. Elicitations tend to work less and less as the targets get older and older, if only because the targets tend to know fewer timely secrets. After retirement, they are often out of the loop, but they may want to prove that they still have it, and this is where the opportunity lies.

4.5.6 Others

The loss of loved ones in any form, births of grandchildren and children, family feuds, serious illness or injury, or other life altering events (or substances) all create opportunities for elicitation and for growing the relationships that are part of that art.

4.6 Tools of influence

Principles and tactics of the elicitation process are based on the concept that the elicitor is trying to produce an automatic response without awareness. These principles and tactics function as shortcuts in decision making. They often operate below the level of awareness and that makes them useful tools that often go undetected. Thus a sound understanding of deception techniques and cognitive processes in people are valuable in the elicitation process. There are other techniques, but these are quite popular because they tend to create automatic responses.

4.6.1 Consistency and commitment

People put a lot of stock in consistency and commitment. They want to be self-consistent and once they have committed they feel obligated to carry through on that commitment. By indicating that actions are consistent with their previous commitments, targets can often be swayed into tracking along with the elicitor.

4.6.2 Reciprocation and sense of obligation

The giving of gifts creates obligations and these obligations are reflected in actions as well as words. If the gifts become excessive too early, they are likely to trigger defensive responses.

4.6.3 Social proof

If 18 million Google hits say so, it must be right. If you look like a member of the group, are with the group, and the group says it's alright to do it, it must be alright. By creating group processes, just like the Internet group process involving multiple identities described earlier, social proof tells the target to go ahead and talk about it. If you haven't seen the movie "*Schindler's List"*, it's worth watching to see how social proof is demonstrated in early scenes.

4.6.4 Authority

Appeals to authority often work, but elicitors have to be very careful because they don't have actual authority, and escalation means dealing with higher level people who are more likely to suspect.

4.6.5 Liking

Obviously the elicitor wants to appear to be the target's good friend and confidant.

4.6.6 Scarcity

The use of scarcity in elicitation is exemplified by asserting that the target is a real expert in the topic and indicating what an honor it is to meet them.

4.6.7 Because

The "because" thing really works, because it generates nearly automatic responses indicating that whatever was said seems like a good reason to follow through with the request.

4.6.8 Contrast effects

The contrast of one situation to another, for example, high gas prices to lower ones, makes the lowered prices seem like they are good when in fact they are worse than the prices before the spike. These sorts of contrasts make it easy to disclose small amounts of information that may be just what the elicitor is looking for.

4.6.9 Presumptive questions

Presumptive questions yield answers in terms of agreement or disagreement that provide the desired information. It is also often easy to tell when someone is being evasive toward answers by the way they answer presumptive questions. Most people also have "tells" that indicate the answer to yes or no questions, even if they don't come right out and answer the question. Tells are very useful to the elicitor, as is body language and other similar behaviors. Using presumptive questions tends to bring out the tells.

4.6.10 Offering alternatives and the illusion of choice

Offering an alternative often causes a correction or selection that is revealing of the underlying knowledge of the target. The illusion of choice is typified by asking someone to pick a number between 1 and 10. When they pick, the magician identifies where to look for the piece of paper where that very number was written down.

4.6.11 Present a paradox at the right time

A paradox can be confusing and, in the right context, provides the impetus for the target to go back to first principles and explain things they otherwise would not reveal.

4.6.12 Question the target's consistency

By questioning consistency, a target can be made to feel like they have to defend themselves by providing additional facts.

4.7 Elicitation in 3 easy steps

Effective elicitation follows a set of reasoned guidelines based on the things discussed throughout this book. A series of steps are typical and listed here.

4.7.1 Step 1: Pick your target carefully

Target selection involves a number of common criteria. In addition to the information above, the following increase the likelihood of finding better targets and choosing when to elicit them...

4.7.1.1 Lower level workers are most susceptible

In a group of workers, lower level ones are more likely to be more susceptible to elicitation, and the lower level they are, the more likely they are. Lower level workers tend to have similar information

in the areas of interest and are also less highly praised, paid, and well treated. They more likely want to impress their peers and feel as if they have worth that is under-recognized.

4.7.1.2 Dissatisfied workers are more susceptible

Workers who are unhappy about their job, who are having problems getting along, who feel challenged by their treatment, who are being left out of the loop on some things, or who are generally frustrated with the workplace are more likely to be less loyal for short periods of time. Those times can be a big problem.

4.7.1.3 Higher level workers are more security conscious

The higher up you are, the more you have to lose, and the more experience you likely have had in terms of losing the battle for secrecy. Higher level workers are given more information about secret issues, are privy to more details of more incidents, and are taken into confidence more often. This makes them more aware.

4.7.2 Step 2: Take your time and use the techniques

The techniques are important because they are the things that exploit weaknesses for benefit. The goal is to build rapport with the target. Rapport building is essential for effective elicitation. It starts by building a "congruence" with the target. By this I mean a set of commonalities that make you seem to them to be similar to them. As was discussed earlier under deception techniques, this includes being like them to be liked by them, the use of similar language and expressions, and so forth.

4.7.2.1 Use mirroring, pacing, and anchoring

Mirroring is behaving just like them in their presence. It includes tilting your head the way they tilt their heads, moving as they move, looking at what they look at. This may seem really strange, but it really works.

4.7.2.2 Let the target lead

Let the target lead the conversation; your job is to sustain it, not to lead it, so they have the opportunity to get to what you want them to talk about. Don't expect too much from the first meeting. In fact, don't expect anything from it other than another meeting, perhaps only a coincidental one.

4.7.2.3 Be patient

Being too focused arouses suspicion. If you walk into a bar, walk up to the target, and say: "Hi, tell me about your nuclear secrets for sex.", it is likely that you will not get any nuclear secrets. The sex is another matter of course.

4.7.2.4 Be a good listener

People that want to tell you about something, want you to listen. They will like you more and be more willing to discuss what's on their mind. Think bartender.

4.7.2.5 Request cooperation in meaningless matters

This process is used to test rapport. As cooperation on meaningless matters becomes successful, the elicitor is ready for the next step. As indicated earlier, a series of small "yes" answers tends to generate more of the same. It is the same with rapport building. As you get more and more cooperation, and as you are a good listener, more and more information will start to come.

4.7.2.6 Get small concessions then larger ones

Attempt to get a small concession first and remind them of it later. This is particularly important when dealing with classified information. There is a subtle art to telling your target that they have already told you about A, so why is B any different. And by extension, C is also no longer taboo. There are, of course, rewards that go with these steps and the rewards increase in value as the steps move on. First it is a bottle of fine wine, then a ski trip, then borrowing the apartment, then helping to pay some tuition in a pinch, then cash in a brown paper bag. As the concessions increase, things will eventually get to the point where the elicitor's requests are uncomfortable.

4.7.2.7 Sink the hook: ask for forbidden things

When the time is right, the elicitor has already extracted significant information that is forbidden, so it's time to move toward blackmail. At this point, the target starts to balk at the request, thinking it is over the top and inappropriate. That's when the blackmailer starts to emerge.

The elicitor, now blackmailer reminds the target that they took money for the last three things provided, that the car they drive and the rooms they are staying in are the elicitor's, and points out the implications of refusing this request. Scandal, possible jail time, loss of their job, loss of the apartment, car, and regular meals, loss of respect from the children, you name it. At some point, there seems to be no way out. Of course there is a way out, and the elicitor can provide it. A life long pleasant existence in a foreign land perhaps? Maybe just one big job a year. Whatever it is, you can bet that a caught fish is only let go once they become inedible.

4.7.3 Step 3: Watch for the problem signs

There are specific problem signs that the elicitor watches for and precautions that they take.

4.7.3.1 Avoid excessive self disclosure and suspicion

The elicitor tells little about themselves. People love to talk about themselves, so they are more than willing to let the elicitor deflect questions. Trying to sidetrack conversation is the next step. If an elicitor cannot reflect back to the target, they can almost always deflect away from themselves. Being evasive or vague in response often works. In summary, the elicitor has to confront the counter elicitation strategy and defeat it or they will end up caught up.

4.7.3.2 Be alert to signs of discomfort

As the target becomes uncomfortable with the situation, the potential for deception increases. At this point it is critical to back off. Specifically, the elicitor should return to an innocuous topic before departing the conversation. People tend to remember what came first and last, so this helps to disassociate the elicitation from the conversation later on.

4.7.3.3 Always create the expectation of future contact

The future contact is the critical component of ongoing elicitation. Without it, the relationship ends and there is surprise if it restarts. The expectation of continuity leads to ongoing relationship building. And even if the elicitor plans to leave, they will not leave the expectation of leaving, lest it would raise suspicion and might get them caught if a trap is being set.

4.7.3.4 The cardinal principle: avoid suspicion at all costs

The elicitor must avoid suspicion until the hook is firmly in place, and if possible, even then. Depending on specific circumstances, the best elicitors may not ever have to force compliance. But when confronted, the elicitor must break off contact. The typical behavior is to simply leave the room, the facility, and the area, perhaps leaving the car off somewhere and switching to a substitute. The elicitor literally must disappear if confronted in this manner.

4.8 Getting them to forget you

This is one of the most important tricks for the elicitation process, so I will repeat it at the expense of boring you. From Karrass, whose work I glossed over earlier, there are some fundamental points that should be noted. Karrass tells us how to get an audience to remember certain things by identifying what is most easily remembered and forgotten in a sequence of events. But the elicitor applies the same principles in reverse to try to get the critical things elicited to be forgotten. Karrass tells us two very important things here.

4.8.1 The first and last things are remembered best

In any exchange, the first and last items discussed will be remembered best with the last being remembered better. That's why elicitors slowly start by saying hello and work their way into the issues they really want to get at. It's also why they always make sure to find a way to end the conversation with a series of things that move the target away from the issues elicited. The theory is that the middle part will be less remembered, and if done properly, it won't be remembered at all.

4.8.2 Repetition enhances memory

The more times something is mentioned, the more it is likely to be remembered. That, for example, is why, in presentations, people are typically instructed to: “tell them what you will tell them, tell them, then tell them what you told them.” The repetition, particularly in different modes, like speech with writing, or pictures with smells, causes better memory and more emphasis. This is also a good educational technique.

So for the elicitor, as soon as the desired information is obtained, it is best to move onto something else, particularly something more interesting and more likely to be remembered. They start and end with more interesting things, don't repeat any questions that are answered, and try to avoid making the things they really want to know obvious or direct.

4.9 The mosaic problem a.k.a. data aggregation

Information comes in small bits and pieces that get verified by other bits and pieces. Our target may say something about a place that they went today and some other target will mention that the buses were all tied up because of the roadwork on the North side of the city, and so forth. Ten or twenty or hundreds of these seemingly unrelated facts may accumulate to indicate that there is a secret weapons plant somewhere working on a particular kind of weapon.

The mosaic problem is one of the hardest ones to solve both from an offense and defense viewpoint and it has been a serious burden on governments for a long long time. Operations security, which I will discuss later, helps to deal with this issue, but it is only poorly understood in terms of solutions, even though the problem seems to be clear.

4.9.1 What is the big picture?

From a standpoint of the offense, the mosaic is a picture that the elicitor is trying to help build of the real situation on the ground. Since nobody knows the whole situation and many people are trying hard not to give information away, the elicitation process is designed to get the big picture by building it up like a mosaic, from small scraps. This typically involves the creation of a table of desired information, the information the offense would have if they knew what they wanted to know. In some cases this is a simple list with general categories while in other cases it is a very long list of specifics. Different lists may be created at different levels and under different plans. In penetration testing efforts, our teams use fairly standard lists of information about enterprises and their decision-makers and workers and we seek out the information using the Internet, databases, and other sources.

As an example, I will use the presence or absence of Weapons of Mass Destruction in Iraq before the 2nd Gulf War, an example that is quite short-term for such an operation, and about which I have no direct knowledge at all. So assume that everything I describe is factually wrong but play along with the story to gain understanding of the issues. You can imagine that there was probably a pretty big list and that many operatives were working hard to get this data from countries all over the world.

4.9.2 What do we know and how well?

After we know what it is we want to know, the next step is to figure out what we actually know and what we don't know. Sounds almost Rumsfeldian doesn't it? That is done by starting to fill in the matrix with known facts, assumptions, guesses, and other information, along with the information on its reliability, source, and method. Once this is done, there is a laundry list of what we don't know, what we don't know well enough to be certain of, and what we know very well or assume. The intelligence process is oriented at filling in the blanks. So we send out our agents, each with their own special territory, contacts, knowledge base, area of expertise, language skills, etc.

4.9.3 What do we need to know and who can get it?

We tell Joe Wilson, for example, that we need to know if Saddam Husein is trying to get weapons grade uranium from Niger. It is now Joe's problem to go to Niger and answer that specific question that fills in his small piece in the big puzzle. And Joe, if he is any good, is not going to James Bond it and drop into a place he has never been in a parachute looking for trouble and telling the world what he is doing. Rather, he will start by contacting old friends who he has known for years and asking them about different aspects of the problem he is trying to solve, each in their own terms.

4.9.4 How do they go out and get it?

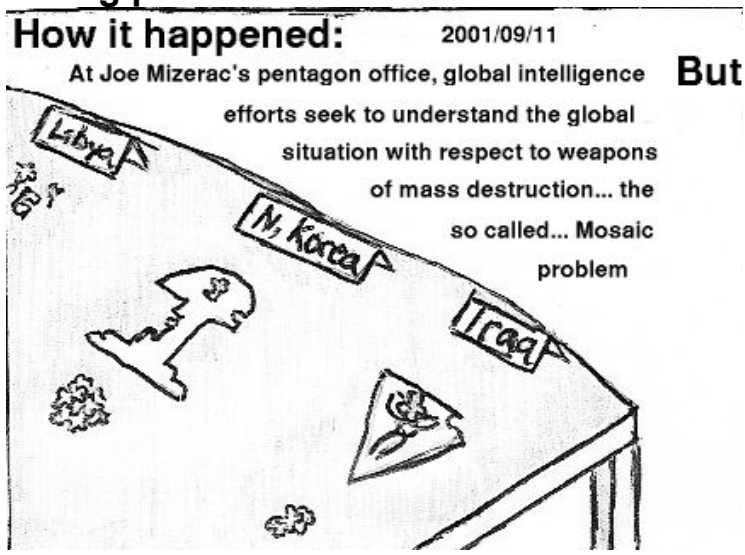
I assume that Joe doesn't just drop into the local mine owner's house and ask "Hey, are you selling enriched uranium to Saddam?" If he were he would likely not tell Joe. Rather, Joe starts to go hunting for information, little bits here and there from different sources, to form the mosaic that will answer the question without

endangering his relationships or otherwise making it harder to come back for him or others. So Joe checks out the local economy and determines that if $10M just entered it, the money disappeared, because in Niger, $10M is so much money it would be impossible to hide. And if there was all this mining, the workers had to come from somewhere, and the folks he knows in the local labor groups don't know of any recent jobs that needed people in the quantities necessary to support the claim. Joe does this for 20 other similar sorts of indicators and starts to fuse the information together into an intelligence assessment of the situation.

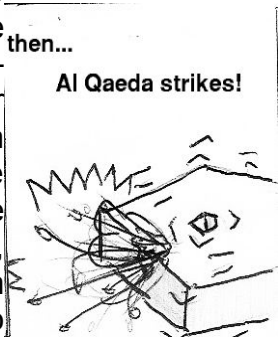
4.9.5 Walking away clean and free

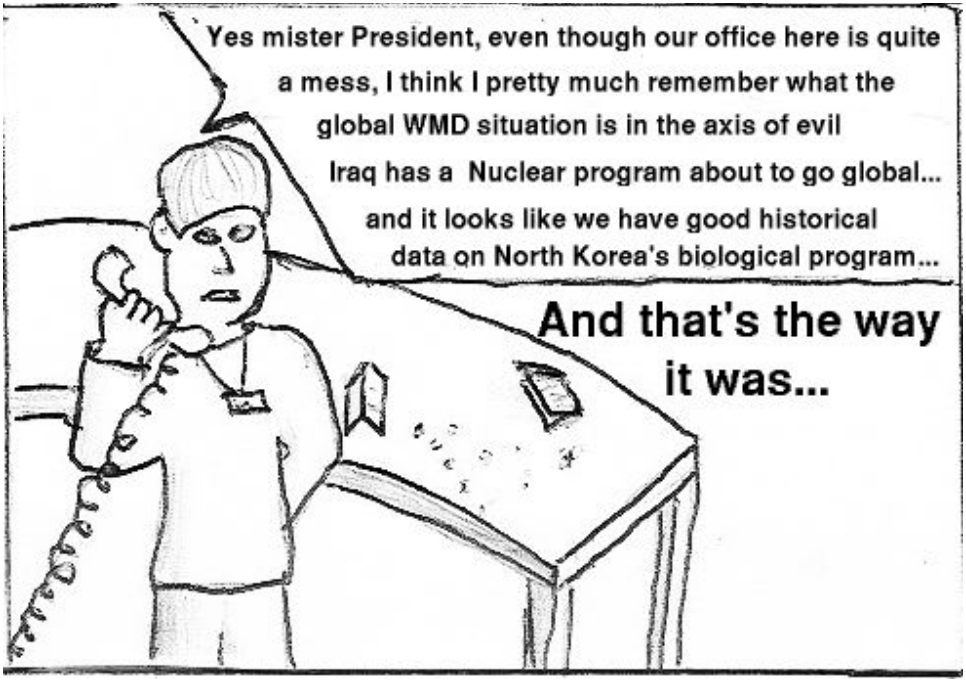
Intelligence assets are not dumb, and they certainly want to walk away free from whatever gathering operation they are on. Presumably this involves having everyone at the end of the day figure you didn't do anything wrong and not understanding the mosaic you built. In Joe's case he wasn't a covert operative, so it didn't matter that much. But for his wife, who was a covert operative, it would likely mean death and dramatic reduction in value of the information and people she ever fostered relationships with. The idea is to walk away clean, an asset for the next mission.

4.9.6 The big picture



At the end of the day, all of the mosaic pieces put together by the Joe Wilsons and Valerie Plames of the world are assembled into the roll-up intelligence estimate that goes to whoever asked the questions in the first place. They can then make decisions from there. And that is the mosaic problem from the standpoint of the offensive. From the standpoint of the defense, the goal is to either prevent the offense from succeeding in their efforts or have them come to defender's desired conclusions, whether they be real or deceptive.





5 Elicitation defense: counterintelligence

Through some oversight in oversight, the word counterintelligence is counterintuitive. That's one of my favorite sentences. Oversight has two exactly opposite sorts of meaning, one being a higher level review and the other being missing something. When oversight reviewed the term counterintelligence they missed something, it was an oversight. Unlike counterintuitive, which means that something is not intuitive, counterintelligence requires a great deal of intelligence. Counterintelligence is about countering the enemy's intelligence efforts. Now that you know how the intelligence operatives do their job, I would be remiss if I failed to tell you how to keep them from succeeding at it.

5.1 Is it a hopeless case?

Can we really expect to win the battle for secrecy in today's world? While it seems clear that controlling the genie of information in general is not feasible, and in fact most readers probably think that more people knowing more is good for all of us, clearly some information should be kept confidential and can be.

5.1.1 Pick your battles

The first step to making a hopeful case for protecting information is to determine what information you really want to protect and how well. In some sense, you have to be ruthless with this selection because defeating elicitation and sophisticated intelligence efforts is very tough and quite expensive in many ways.

5.1.2 Make a plan

The old saying goes that any plan is better than no plan. But in countering the intelligence threat, any old plan just won't get the job done. For elicitation tactics, the only effective plan involves intensive employee training and awareness at all levels for all employees that potentially could access the information you are trying to protect. This goes hand in hand with technical controls.

The typical counterintelligence plan involves training people to recognize elicitation, preparing effective on-the-spot counter-elicitation tactics, having an effective reporting system for detected

incidents, building an investigative process for the elicitation process, and once the source has been detected, preparing an effective process to defeat, deter or deceive further efforts.

5.1.3 Execute the plan

Once you have a plan, you need to execute it and execute it well. Unlike trying to defend against casual attackers, countering serious intelligence threats has to be done at a professional level and on a full time basis.

5.2 Recognizing elicitation

People without an intelligence process or desire to get secret information can also be friendly and likable. They might want to get to know you because you are a nice person or because they like the way you look. If you become excessive in your zeal to detect elicitation, you will likely never get married or have kids or make friends or anything else.

5.2.1 Is it honest normal human interaction?

Recognizing honest influence and normal friendliness is not all that hard to do, but there is no guarantee that even the person who is just being friendly doesn't want to get something from you - like friendship back - or you to donate money to their favorite cause - or great sex - or a spouse - or whatever else. The question you have to ask yourself is what you want out of the relationship and what you can reasonably expect from someone that would want you to have that.

5.2.2 Are you famous, rich, or a hunk? Really!

For example, if you are 50 years old, over weight, not Steve McQueen or even Dustin Hoffman, and an 18-year old girl with a slender body and flowing blond hair approaches you in a friendly way as if she were attracted to you, and she is not selling you something or working as a paid consort, the odds are that her interest is not in your best interest.

5.2.3 JDLR

This falls under the JDLR rule. JDLR is an abbreviation used by police all over the world. It means "Just Don't Look Right". If you have any kind of sense at all, you will find lots of things that meet

the JDLR category in your life. If you have a secret to keep, you should avoid them unless you are an investigator in which case you should investigate them. I do not mean it as an insult to middle aged men when I tell them that 18 year old beautiful women are not really attracted to them. And by the way, the same applies to most middle aged women who hold classified data, have just been divorced, and are approached by far younger men. Except of course that most men are indeed attracted to almost any woman some of the time. But that aside, it fits into the JDLR category.

5.2.4 Why would they want to talk to you?

So much for the sex approach. Obviously the other approaches are harder to ferret out, but they are also fairly identifiable. For example, when someone from North Korea or Iran or Big Bad Country approaches you and their country is listed as a country considered an enemy of your country, (it changes so keep watching the list), assume that it is part of an elicitation effort.

When I was working indirectly for the US government, I was once approached by someone from such a country who a friend told me was an intelligence operative. Of course I didn't particularly believe it, but what could I do but report it? I went to my friend because I thought the contact was a bit strange. But more on this story later.

5.2.5 In reflection

Another hint that elicitation is taking place is that, usually on reflection, you feel like you might have said something important during the conversation, but you are not sure what, and you feel a bit uncomfortable about it. Another hint is that over a period of many conversations, work-related topics keep coming up when you don't work with the individual. Of course if they are good they are trying hard to avoid making their efforts apparent, so it will be a challenge. As a rule of thumb, when there is doubt, present it to an independent authority for their review. This will be your counterintelligence representative. But I am getting ahead of myself.

5.3 Countering elicitation

Countermeasures involve a "battle of wills" rather than a "battle of wits." It doesn't take brilliant people to defeat these tactics, it just takes enough resources applied in the right ways, attention to detail, and investment in training your people on what to do.

5.3.1 On the ground

When you are chatting with someone and start to become suspicious that they are an elicitor, you don't have the luxury of going for help. You have to react on the ground to the situation you are in.

5.3.1.1 Avoid the question if possible

The most simple and obvious move is to avoid the subject if it gets near anything that might be the subject of elicitation. Just move on to some other subject.

5.3.1.2 Make a joke and change the subject

Making a joke is a good way to move on. "If I knew about that, I sure wouldn't be here!" or "That's above my pay grade." are reasonable. Changing the subject, if overly abrupt, can signal suspicion, and that should be avoided.

5.3.1.3 Use the memory jogger gambit

"That reminds me of..." is the key phrase here. "You know, that reminds me of the time I went fishing back in Iowa and caught a huge Bass without a lure. The strange thing is, they said they wouldn't have Bass in that lake and ..." Try to be reasonably intelligent about your choice of what it reminds you of.

5.3.1.4 Avoid the tendency to "set them straight"

If they are wrong, you might try to simply let them be wrong. Or you might just act like you haven't a clue about what they are saying to you and tell them you never thought about it that way.

5.3.1.5 Use your partner to bail you out

You do have a partner - don't you? If not, what do you think you are doing there all alone in a strange place with this elicitor?

5.3.1.6 Misunderstand the statement or question

"Huh? I'm sorry, I must be having a senior moment... what did you say?" Or this one: "I had one of these when I was a kid." I know - it makes no sense - but then you misunderstood them and heard something about a sled, not the type of lead.

5.3.1.7 Avoid displaying sensitivity to "hot buttons"

Get a grip. Remember, people are starving in Africa. So whatever the hot button was they were trying to push, it's not that hot.

5.3.1.8 Always distrust the environment

Don't be paranoid... but they **are** out to get you! I will return to this.

5.3.1.9 Always return to your "circle of comfort"

If something makes you uncomfortable, try to return to thoughts and areas where you are comfortable talking. Just redirect your conversation toward another issue, or tell them: “I'm getting bored. Enough of work for now. Let's talk about the game. Did you go?”

5.3.1.10 Familiarize yourself with elicitation techniques

Read the last chapter if you didn't do it already, and understand what the elicitor is doing and why.

5.3.1.11 Prepare directed responses

Be prepared - the Boy Scout's motto. If you get a question about secret information, you should already have thought through the responses you will give, and have them ready to go. I find it a lot easier to think quickly if I have already thought through the issue.

5.3.1.12 Develop a repertoire of evasive responses

Practice makes perfect. Build up a library of weird jokes or clever responses or alternatives listed here and use them if and when you have to. Practice on your kids when they ask for the car keys.

5.3.1.13 Avoid being isolated or excessive

The best way to not get shot is to not be where folks are shooting. In other words, if you think ahead, you are less likely to be in situations where you can be elicited easily. Remember the partner thing? Why are you going out to a bar in Bucharest with the new acquaintance from the conference and nobody else? Don't you know from watching young women at bars that you always travel in packs if you are trying to stay safe? If you get completely drunk in

the middle of a strange land, why do you expect that nobody will try to take advantage of you. I would call it common sense, but it's not that common.

One of the more interesting stories of elicitation strategy practiced by the Russians for some time involved a spot out of the normal tourist areas where folks on special assignments were posted. These folks were welcomed by the Russians for their stay of however many weeks or months by being brought to the local bar. At the bar, the only place to go after work, they would meet a Russian KGB representative who would tell the Americans that he was from the KGB and that it was his job to try to get them to reveal information that was classified. He would ask them if they wanted to give away any secrets in exchange for money, they would say “no”, he would indicate that the girls at the bar were there to "entertain" the guests, and everyone would sit down together, drink, carouse, and generally have a good time. This would be reported as meeting the requirement by the KGB folks, reported to US counterintelligence, and that was the end of it.

Except of course that the Russians were not as dumb as they looked. The process actually produced plenty of friendships and lowered the guard of the Americans to allow elicitation in its more subtle form to take place. You catch more flies with honey.

5.3.2 Report it and find out

If you think you have been elicited you are supposed to report it to counterintelligence so they can determine what you should do next and generally follow up with countermeasures. Which brings me back to my story.

My elicitor was promptly reported as he was supposed to be. My counterintelligence person indicated they would get back to me... and they did... six months later. I was introduced to a gentleman who validated my suspicion and told me that I should decide how to proceed on my own. In other words, it took six months to tell me to do whatever I thought was best. I guess I figured they would want me to carry out some intriguing program sending false information

or creating a relationship so they could exploit the bad guys. Nope. Just make up my own mind. So I decided to disengage, not that all that much engagement was likely to happen after six months of ignoring the foreign agent or delaying any action.

5.3.3 The counterintelligence plan

There are a number of reasonable options for countering elicitation beyond the tactical responses indicated above.

5.3.3.1 Just ignore it

The likely reasons that I was not engaged in some international intrigue is that nobody had any particular interest in protecting the unclassified program I was engaged in, that the agent was only asking to purchase a book that was available over the Internet to anyone unless they were from somewhere that I was not allowed to ship any goods, and that if I could figure it out by chatting with the guy, he wasn't likely to be all that effective a foreign intelligence agent. But of course that is not always the case.

In truth, as long as you can identify the elicitation effort and effectively prevent leaking information, you have won. They waste time and effort and don't get anything of interest. The fact that they wasted time on me seems to indicate how far off target they must have been. And frankly, it costs a fair amount to do something like this and unless there is a good reason to do it, why bother.

5.3.3.2 How about a deception

The obvious thing to do to counter intelligence efforts is to carry out your own deception by providing false information. But this sort of operation is a bit tricky. In particular, you need to have some plan in place for what to provide the enemy elicitor. And if they are going to take the bait it probably costs a lot to run the deception program. Remember, they are building up a complex picture and if pieces don't fit, they may well start to see a patten of deception and determine what you are doing. And if there is another program in place you might risk bumping into each other. All of this is why counterintelligence is coordinated at a strategic level, ultimately involving a more or less central committee that determines what operations to carry out.

5.3.3.3 Just track them and look for changes

An obvious tactic is to track elicitation behaviors as reported and look for changes in those behaviors that would tend to indicate that the enemy has changed tactics. This could indicate that they found something, that they realized you were tracking them, and so forth. Of course you have to figure out which or you will never know what's really going on. Better start eliciting. Isn't the spy game fun?

5.3.3.4 What if it was a ploy?

There is always the possibility that the whole intelligence effort and my reporting of it was just a test to see that I was following the rules. After all, countering intelligence relies on having trusted people with your secrets. But maybe I was supposed to think it was a ploy. OK, so this eventually gets us to the problem of layers of deception. How deep is it anyway? And who would know? And if they told you, how would you know the answer was the truth?

5.4 Operations security

The most important approach to defeating enemy intelligence attempts is to have effective operations security. And it turns out this is also useful for other sorts of operations, from corporate operations to police actions and investigations.

5.4.1 Who needs it and when?

An operation is any activity that is being carried out that needs to be protected. So if you are doing something that needs to have some sort of protection, you should use operations security, or as it is called in the trade, OPSEC. When might you need OPSEC?

5.4.1.1 A corporate example

If you are trying to merge two companies and don't want anybody to know until the public announcement in order to protect the shareholder value and remain legal, you might need OPSEC.

5.4.1.2 A police example

If you are running a policy operation where you set up a phony storefront that is selling supposedly stolen goods, and you need to make sure that it looks like what it portrays in order to protect the lives of the police involved and have a successful operation, you might need OPSEC.

5.4.1.3 A penetration testing example

Another example is penetration testing that some of my group's assessments do. In this case, we have to make sure that our people are not put at risk by providing adequate protections of their health, safety, and well being during the operation. If your people are potentially at risk in an operation, you might need OPSEC.

"You might be a redneck" ... "You might need OPSEC" ... it rhymes

5.4.1.4 An intelligence gathering example

In some of the intelligence gathering operations I have run, the requirement was that the people we were gathering intelligence against must not be aware of who we were working for or the real purpose or nature of our efforts. If these folks knew what we were doing, they might have wanted to kill us to keep us from delivering our results... they are pretty nasty folks. If you are gathering intelligence on bad guys, you might need OPSEC.

5.4.1.5 A surprise party example

Suppose you want to have a surprise party for someone you live with. In this case the idea is to make sure that the party gets set up without the person being surprised finding out about it or suspecting anything. If you're keeping a secret from your significant other, you might need OPSEC.

5.4.2 Some common threads

Operations have some common threads that lead to progress in the OPSEC problem.

5.4.2.1 Limited time frames

Operations generally last for finite time periods and in most cases these periods are not very long. Weeks, sure. Perhaps months. Sometimes years. But not forever. For that reason they have a beginning, a middle, and an end that are reasonably well defined.

5.4.2.2 Limited scope

Operations are often against some individual or organization and this provides the potential to understand enough about the threat to be effective at defending against it. Thus the operation doesn't have to be defended against everyone from everywhere.

5.4.2.3 Limited secrets

Operations generally have specific things that are confidential and others that are not. As a result, not everything has to be protected. That means you can focus your resources where they are needed.

5.4.2.4 Simplification

So in summary, we want to protect some specific things against some specific threats for some specific time period. This greatly simplifies the problem as opposed to generally protecting everything against anyone forever, which is impossible. Generally, if you have an operation that has any secrets or risks, you most certainly do need OPSEC.

5.4.3 What gives it away?

It is worth noting that little things give away operations. It is this attention to detail that makes OPSEC work.

5.4.3.1 Indicators

For example, if you are having a surprise party, don't leave receipts from the purchases on the charge card unless the bill won't be there until after the party. If you leave a wrapper in the garbage and the target of the surprise takes out the garbage today on a lark, they may notice the party wrappers, realize that their birthday is coming up, and suspect. Or in the parlance of the class I spoke to today, you are hosed! They dared me to put it into my next book, and I am a chump for a dare. Actually I am not, but I figured that by putting it in they would figure I was. Of course having told you that, I guess it loses its purpose, if they read the book... It's the little things that give you away. These are called “indicators”.

5.4.3.2 Identifying indicators

What are those little things? How do we make sure we don't miss any? Everything that anybody ever does can be thought of as a process. Processes have sequences of activities that involve people, things, money, times, locations, and so forth. To do a proper job of identifying the little things you need to understand the normal process and the process of the operation and depict the normal process as if it were unchanged while depicting the operation as if it was what you want it to be perceived as.

5.4.3.3 An example indicator for surprise attack

Think about deliveries of pizza to the pentagon whenever a surprise attack is about to take place. Then think about ordering pizza at the pentagon when no attack is coming to make the enemy doubt their intelligence. Then think some more.

5.4.3.4 Don't forget the big things

Oh. I forgot to mention it. The big things can also give you away. So watch them too.

5.4.4 The five phases of operations security

OPSEC is a process for identifying, controlling, and protecting information that an adversary could exploit to the defender's disadvantage. It generally happens in five phases.

5.4.4.1 Identify what has to be protected

The operation is finite, so we might be able to identify what is important to protect over that time period.

5.4.4.1.1 Different strokes for different folks

For example, in gathering information on a criminal gang, we probably don't want them to suspect that we are doing it or be able to figure out who we are. If they do suspect, the consequence could be the death of the investigators and loss of the benefits of the operation. On the other hand, for a surprise party, we usually need to protect against knowledge of the existence of the party, of the people participating, of the location and its preparation, and indirectly, against finding or understanding clues that would make the situation look suspiciously like a surprise party to the target.

5.4.4.1.2 Building systems for secret uses

In one case we were building computers for use in classified data processing. One concern was that an intelligence agency might plant hardware to leak information if they knew these computers were used for this purpose. We identified the purchasing process as a possible problem, so we purchased parts for these systems along with other parts used in larger volume for other purposes, and associated these purchases with different accounts than the classified systems. We then made internal transfers to fix up the bookkeeping to accurately reflect the financial situation.

5.4.4.1.3 A sting operation

For a sting operation, we surely would not want the criminals to know that the people in the storefront were police, so we would want police that were not known to criminals in the area. In other words, the police on the streets of the city every day might be easily recognized, so we will have to use a different group. And if they are supposed to go home at night, they better have a place to go where they can be followed, at least if any serious criminal organization is the target. Where does the money go? Where do the goods come from? Where did the proprietor come from? Do they know the business they are in and what to charge and pay for what? Do they wear the right clothes, speak the right language, drink the right beverages, drive the right car or take the bus? Do they act in every way like what they claim to be?

5.4.4.2 Determine adversary intelligence capability

Who might want to find out these things?

5.4.4.2.1 Who are they?

Is it just the target of the operation? Probably not. For example, in the sting operation, what about the competitor criminal fences? They may be motivated to find out what's up. How about the landlord? The neighbors? Those sincere bystanders that just want to help may endanger the whole operation if ignored? And back to the surprise party, suppose someone that doesn't know about it sees someone shopping for balloons and mentions it to the person to be surprised. What is the cover story?

5.4.4.2.2 Identify capabilities and intents

Once the adversaries are identified, their capabilities and intents are analyzed to identify what techniques they might use to gain access to the information that has to be protected in order for the operation to succeed. The landlord has access to bank account information associated with rent checks unless rent is paid in cash. They may be able to come into the back of the storefront using a landlord key, or they may have a surveillance system in the building and the capacity to record conversations in the back room. The criminals that are being hunted may be gangs with some level of computer savvy, they may use private detectives or bribe people at

the department of motor vehicles to get information on team members, they may follow workers home to check them out, they might ask around on the street. Some gangs have reasonably sophisticated surveillance capabilities and some break into computer systems. Whatever their capabilities are, they have to be identified, along with the methods they use to get information using these capabilities.

5.4.4.2.3 What indicators can they observe?

Many intelligence operations:

- review widely available literature,
- send intelligence operatives into adversary countries, businesses, or facilities,
- plant surveillance devices (bugs) in computers, buildings, cars, offices, and elsewhere,
- take inside and outside pictures on building tours,
- send emails in to ask questions,
- call telephone numbers to determine who works where, and to get other related information,
- look for or build up a telephone directory,
- build an organizational chart,
- cull through thousands of Internet postings,
- do Google and other similar searches,
- target individuals for elicitation,
- track the movement of people and things,
- track customers, suppliers, consultants, vendors, service contracts, and other business relationships,
- do credit checks on individual targets of interest,
- use commercial databases to get background information,
- access history of individuals including airline reservations and when they go where,
- research businesses people have worked for and people they know,
- find out where they went to school and chat with friends they knew from way back,
- talk to neighbors, former employers, and bartenders,
- read the annual report, and
- send people in for job interviews, some of whom get jobs.

5.4.4.2.4 What should these indicators look like?

Going back to the storefront example, try making a list of what you imagine a criminal gang might do in this context to get an idea for what to look for as indicators. Also consider that these operations may get suspicious if very little information is available. And they might also check out the references you give, not just check with them. Consider the possibility that the adversary is a professional with extensive training and substantial money and access. Obviously this varies for different sorts of operations, based on the identified threats. Is your spouse going to use the private detective they have tracking you to find out about the surprise party? Are you going to invite the private detective to come to the party? That would be a surprise! Threat assessment is a professional activity carried out by experienced professionals that spend their lives doing it.

5.4.4.3 What are the vulnerabilities?

The next step is to think about how each of these things might be done by the adversary, and to start coming up with how doing these things might get them the information you are trying to protect. This is not limited to direct actions, like knocking on the front door and asking if you are a police operation.

5.4.4.3.1 How do the threats observe and process indicators

People who spend their lives working on these issues understand vulnerabilities far better than those who read about them in the paper. Threats tend to use the full spectrum of possibilities. More sophisticated threats use more of the spectrum and do so far better, more carefully, and over longer time frames. My teams sometimes use checklists to get our experts started and to make sure they don't miss anything, but most of them walk up to a facility and look for “rat droppings”. We use that term because when you see rat droppings, you know there are rats, even if you don't see the rats. Are there cigarette butts by an outer door? This an area where employees go outside the building to smoke during breaks! Fences don't usually observe smoking rules. Crooks will think this is not a real fence. After you identify the issues, you need to go back and check your work.

5.4.4.3.2 Attack graphs and getting indications

A method that my teams use for analyzing vulnerabilities in high consequence situations is to create attack graphs. These are built up from lists of individual weaknesses found in each aspect of the operation, and combined together to identify all possible sequences of their exploitation. We then identify paths from the source of the attack (each threat) to the destination (the information we want to protect). Part of the process includes the notion that instead of seeking answers, the adversary may simply guess them. If the adversary guesses right or wrong, can they tell? For example, if I want to find a data center in a building, I don't have to find something with the label "data center" on it. Instead, I might look for lots of air conditioning and guess that it is feeding the data center. If I am wrong, could I tell by shutting down the air conditioner and seeing what the response is?

5.4.4.4 How serious is the risk?

Now the magic happens. The decision maker who is in charge of the operation and has responsibility for (or is directly affected by) the consequences of its failure has to make a decision. Is the consequence high enough to justify added countermeasures?

5.4.4.4.1 The magic of risk assessment

When I say "magic happens", I am not kidding. There is no well defined process for making these decisions. There is usually just the decision maker's gut feeling, augmented by the information generated by the process described above. Do you feel lucky? If so, take more risks. If not, don't, and spend the money, time, effort, etc. to mitigate the risks.

5.4.4.4.2 Who decides?

Unlike most risk management, OPSEC generally assumes that the operation will take place. But in the end, just like other risk management areas, risks can be avoided by deciding the operation is too risky and not doing it. If this decision cannot be made by the risk manager, they should not be the risk manager. For the US in military operations, the President is the risk manager. For police operations, it's usually a captain or commander. For a surprise party, it is usually the spouse or parent.

5.4.4.4.3 What do they decide on?

The selection of countermeasures is also embedded in this process and the cost is normally borne by the decision maker or their organization. In this sense it interacts with the next phase, going back and forth until the risk is adequately managed.

5.4.4.5 Identify and apply countermeasures

The last step, and it interacts with the previous step, is to identify what to do about the risks. In general, countermeasures are mitigation strategies intended to reduce the chance and/or size of the consequences.

5.4.4.5.1 Make it look real

Returning to the example, the landlord who rents the storefront has to see it as completely "legitimate" in the sense of being a storefront set up for the sort of business it is in. So it has to be in the right kind of neighborhood, the lease has to be for as long as most such leases are, the same sorts of haggling has to be done over painting the walls and the water not working right in the bathroom, and so forth. Rent should be paid through fictitious accounts set up for the fictitious identities of the police officers, and the accounts should not be magically filled with money. A cover story is needed for the reason the operation moved in, and so forth. But maybe the risk manager decides to mitigate the risk by paying cash for rent and telling the landlord "We won't report it if you don't". Most sleazy landlords will take cash for rent, and if you don't want a receipt they will be happy not to give you one, even if they are completely legitimate and report all of the income on their taxes. If not, bust them as the operation ends.

5.4.4.5.2 Focus on key indicators

The idea of countermeasures is to disrupt the ability of the adversary to collect the information you want to keep them from getting or keep them from understanding what they do get. In other words, you want to control the opponent's indicators. So the crooks decide to follow the cops home to see if they are legitimate. The cop pulls up to a modest apartment with a security door, drives into the underground garage which is protected by an automatic door, and disappears for the night. As long as the crook can't tell the cop

is a cop, it may be adequate for the needs of the operation. If they check the landlord, the rent is paid in cash in advance month by month and they have been here for 3 weeks. No phone is installed, they seem to watch television and order out for diner - mostly pizza and Italian sandwiches. Sometimes they go to the restaurant around the corner. On weekends they leave and don't come back till Sunday night. Simple, inexpensive, and defeats almost all attempts within the capability of the typical crooks while leaving proper and consistent indicators to avoid suspicion of concealment.

5.4.4.5.3 Threats imply indicators

But suppose it is a foreign intelligence operation. A fingerprint database is likely kept on folks, so changing a name will not work. They can probably gain access to the US fingerprint databases used for criminal investigations, so anyone you put on the job has to be someone that has a deep cover. It probably takes many years to create this cover and costs many millions of dollars. They might go to graduate school in the foreign country and get to know other students through that process, befriending them and becoming part of their lives over many years. Again, the set of things that need to be done grows with the threat capabilities and intents and the nature of the information being protected, because the indicators and analysis capabilities grow with increasingly capable threats.

5.4.4.5.4 Keep it as simple as possible

As a rule, the best countermeasures are simple, straightforward, and inexpensive. When you get fancy, you find that the complexity builds and becomes unmanageable. A consistent story that holds up all the way to the bottom is what you need. This means using as few lies as possible, because it is so hard to keep all your lies straight.

5.4.4.5.5 But no simpler

Simple is good, but adequate fidelity to the need is critical. If you get too simple against a capable adversary, you are likely to be defeated. But in the end, you have to make decisions and you have to stop somewhere, so experience and judgment end up forming the magic components of risk management.

5.5 You're not paranoid, they are out to get you

The definition of paranoia is **unrealistic** fear that "they" are out to get you. But not all fear is unrealistic.

5.5.1 Distinguishing between paranoia and fear

The way to tell the difference between fear and paranoia is to get a realistic grip on the reality of the threats. This book tries to help understand threats by characterizing what they do and giving facts about them. But just because there are real threats, doesn't mean you are not paranoid. When you let fear grip you to the point where you stop doing the things you want to do with your life, you are likely to move toward paranoia. But when you overcome your fears and do what you want to do despite them, the fear dissipates and you become able to function.

5.5.2 They really are out to get you

I told you I would get back to this. They are out to get you. Just look at them. The terrorists, the war mongers, the fraudsters, the scam artists, all of those people sending all of that spam email, the fake Web sites, the telephone solicitors... but not everybody you meet. In fact, only a small portion of them. Most people are friendly.

5.5.3 Don't live in fear anyway

OK, the world is not safe, and you and I are both going to die. "Nobody gets out of here alive!" By definition, you can't get out of life without dying, and living forever would get boring anyway. My advice is to choose life! Don't do stupid things, don't take unnecessary risks, don't walk into machine gun fire or go to the middle of areas where people are being slaughtered unless you want to do that for a living and have proper training and experience to do it in relative safety. I am learning to SCUBA dive. It's fun. But without proper training and care you can die from it. So get trained!

5.5.4 Knowledge is the answer

In the end, I believe that the solution to understanding risks rationally comes from knowledge. The more you know, the more you have experienced, and the more you study what you do, the better you are likely to be at it.

5.6 Defeating data aggregation

I discussed the mosaic problem earlier, and I thought I would revisit it here for just a bit because it is so important and so tricky. The problem is that data from many sources can be aggregated together, fused, analyzed, and presented so as to be understood in context. This leads to knowledge that may be the very secrets that the spies are trying to get and the OPSEC people are trying to protect.

5.6.1 The end of privacy?

It's an uphill battle to keep secrets, especially in today's world where the Internet makes so much information so readily available, where large databases grant access to so much data about people, where there are pictures taken in the surveillance nations at street corners, in shop after shop, in hallways, in restaurants, and in bookstores. In most cases, there is enough data out there and potentially available to track people for very significant portions of their lives.

5.6.2 No threats have all sources... yet...

The good news is that no one source really has access to all of this data or the capacity to analyze it all. On the average, you are not likely to be found unless someone is looking for you, and if someone tries to hunt you down by tracing your movements, they will have a hard time getting access to all of the necessary footage unless they are very public about trying to find you, or you are in China or Singapore. As the intelligence effort footprint gets deeper, the likelihood of detection increases, and most intelligence operations try to be relatively covert. But that need not be true.

5.6.3 Surveillance nation?

Most people in the United States today use credit or debit cards for most of their financial transactions, and checks or direct bank transfer payments for many of the rest of their transactions. Cash is less and less a part of the economy and yet cash is the only relatively untraceable monetary transaction process available. Follow the money and you get to many interesting pieces of information. Will yours become a surveillance nation? This is the problem, and the world is looking for the solution.

6 Countering frauds

Given the understanding of high-level intelligence efforts, cognitive weaknesses and how they are exploited, and how high-level counterintelligence works at a simplistic level, you might think that you could readily counter frauds well. And indeed these things help.

But some of the smartest and most widely respected people in the world, including ex-counterintelligence workers, get defrauded. That's because we all have moments of weakness. Perfection is not possible and is not the target of my efforts in this book. Rather, the strategy that I believe is effective for countering frauds is a mixed approach that starts with gaining control over your life and over your mind. Knowledge is power.

6.1 Countering corporate frauds

Corporations counter fraud on large scales by using widely known and long used principles to prevent frauds and abuse, by a mix of prevention, detection, and response, and through a good internal audit and investigative process.

6.1.1 GASSP

The "*Generally Accepted Information Security Principles*" (GAISP) and the "*Generally Accepted Accounting Practices*" (GAAP). are good examples. GAAP accounting should be followed by all large companies and is legally mandated for most public companies. GAISP and its predecessor GASSP (Systems for Information) include the following relevant items. More details are available on my Web site (http://all.net/) under "Protection Standards".

6.1.1.1 Accountability Principle

The accountability principle basically states that people should be accountable for their actions. In other words, what people do should be attributable to them. This means that if someone tries one of the many frauds described earlier, there will be a clear accounting of what they did so they can be prosecuted if found. They should be aware of this so that they will be less likely to try.

6.1.1.2 Awareness Principle

The awareness principle says that workers should be aware of the security requirements placed upon them, of their accountability for what they do, and for the potential consequences to the company and to them of perpetrating attacks, including frauds. This will help to deter the 1/3 of employees who might commit frauds if they thought they would not get caught.

6.1.1.3 Ethics Principle

The ethics principle says that the company should be ethical to its workers and that standards of conduct for ethical behavior by workers should be provided to those workers. This will help to convince the 1/3 of employees who may be willing to defraud the company not to do so because the company is being fair with them.

6.1.1.4 Multidisciplinary Principle

The multidisciplinary principle states that security involves a wide range of disciplines that have to work together in order to provide effective protection. In terms of frauds this means that preventing, detecting, and reacting to frauds involves a team effort and that many people are involved in the process.

6.1.1.5 Proportionality Principle

“Let the punishment fit the crime” is an example of this. But another example is to put forth more effort on things that are more costly to the company. So people taking home pencils from the company when they are mostly used up are probably left alone while people who can take millions of dollars or more should be watched far more carefully.

6.1.1.6 Timeliness Principle

This principle states that when more damage can be done sooner, the defense process has to be faster. So the detection and reaction to a smash and grab scheme should be fast enough to catch the thief before they get away, while the reaction to a "long con" can be slower and still be effective. Since it costs more to react faster in most cases, companies can save money by not going as fast as possible all the time. For example, quarterly financial system reviews might work against payroll frauds while electronic funds transfer frauds may lose too much too fast for this sort of delay.

6.1.1.7 Reassessment Principle

This principle states that risks should be reassessed periodically or when things change significantly. So the fraud detection scheme for financial frauds should be reviewed whenever the financial system changes substantially and every year or so because the fraudsters come up with new ideas over time. If you are in a financial services company, you might do this quarterly because frauds are changing.

6.1.1.8 Internal Control Principle

This principle says that a set of internal controls should be in place so that when people try to defraud you, the controls prevent high valued losses and detect and react to lower valued losses before they add up. Controls include things like limiting the largest amount allowed to be paid on a company check, requiring approvals for purchasing or inventory changes, and locking up the trash areas so that people can't dumpster dive.

6.1.1.9 Adversary Principle

The idea here is the same as the one from OPSEC. You should consider the adversary when designing your defenses. If you are in the national security business you face different adversaries than if you are in the greeting card business. You should not prepare for spies if you face only fraudsters.

6.1.1.10 Least Privilege Principle

The principle of least privilege is based on the idea that if you don't need to be able to do something in order to do your job, you should not be able to do it. For example, if you are not in purchasing, you should not be able to create purchase orders. This keeps people from abusing access beyond the access they are granted to do their jobs.

6.1.1.11 Separation of Duties Principle

Separation of duties is used to assure that individuals cannot cause more than a limited amount of harm. Thus, whether through mistake or abuse, no individual can both create a purchase order and make a payment against it. This keeps individuals from being able to cause harm on their own. So it takes a collusion of at least two people to take advantage of the system, or at least the passive participation of one of them.

6.1.1.12 Continuity Principle

The continuity principle says, in essence, that the business has to continue even if things fail selectively. That means that no person is so important and no system is so vital that the business cannot go on without it. This cannot be the case in most really small businesses but as businesses grow this can often be the case and should be.

6.1.1.13 Simplicity Principle

As Albert Einstein said when referring to a good theory of the Universe, it should be "As simple as possible but no simpler". The simplicity principle says that security measures should be that way too. Don't use complicated solutions when simpler ones will do.

6.1.2 Other general issues

Some of the other general principles that are not codified in historic standards but that should be considered by companies are included here before I get into specifics.

6.1.2.1 Who works for who?

Many corporate officers don't seem to get it. They work for the shareholders and not themselves. This is something that has to be made very clear by shareholders by being better represented and more present. For private companies the shareholders have to get personally involved. For public companies the board of directors represents the shareholders and must be held personally accountable for doing that job well. And in case you didn't know it, employees work for the company, not for their bosses. And the folks at the White House work for the country, not for the President.

6.1.2.2 Contractual limits

Employee contracts need to include proper provisions for fraudulent behavior, and that includes contracts for top executives. Personal liability and criminal prosecution should be guaranteed for anyone who cooks the books. If you can''t get an executive under these terms, call me up. I know plenty of honest hard working competent executives who will likely do an outstanding job for less than the millions of dollars some executives get paid today. You can do better if you try.

6.1.2.3 Follow through

This is where most companies really fall over. When an officer violates the trust of the employees they need to get prosecuted criminally and sued personally by the company and by the people who were defrauded, the shareholders. The names of criminals should be widely published when found guilty so that the whole world knows and the shame falls on them and their family.

6.1.2.4 Cover ups should be punished harshly

I cannot tell you (I am quite literally barred from doing so by the confidentiality requirements in contracts) how many times we track insider abuses down to executives that never result in prosecutions or even terminations. These criminals are often retained and continue to do harm. They may move on to other victim companies without negative reputations or bad recommendations because the company they stole from has some perceived liability associated with giving negative recommendations.

6.1.2.5 Liability should be put in for failure to warn

I think that legislatures should make laws that state that failure to warn employers of frauds when they request recommendations introduces liability for all of the costs and consequences of future frauds to subsequent employers. And there should be no liability for giving any opinion you want to give when you are asked for a recommendation on a former employee unless you can be proven to have lied about it.

6.1.3 Deter, prevent, detect and respond, and adapt

The typical defense process consists of deterring frauds, preventing them where feasible, detecting and reacting to them when they occur, and adapting the overall business so as to reduce them to acceptable levels over the long run. A perfect system does not and likely can not exist, but if it did, it would likely cost so much that it would be a poor business decision to put it in place.

6.1.3.1 Deter

Deterrence works on people who would not perpetrate a fraud if they were afraid they would get caught. The idea is to make them think that the odds of getting caught are high and that the punishments are likely to be severe.

6.1.3.2 Prevent

Preventing frauds consist largely of implementing combinations of controls. Controls consist of things like approval requirements for purchases and reconciliation processes before payments. By making more than one person get involved in a transaction, it becomes harder for individuals to succeed. Most insider frauds involve individuals, perhaps acting in concert with outsiders. As the consequences increase, more controls may be required. Another sort of control is preventing functions that don't need to be done from ever being done. For example, cash transactions have been largely eliminated for many businesses, thus reducing the potential for any sort of fraud involving cash and reducing risks.

6.1.3.3 Detect and respond

Detection and reaction go hand in hand. If you can detect something but can't react in time to prevent serious harm, it may not be worth the time and effort to detect it. And of course you cannot react sensibly if you don't detect. The question is what to detect and how to do it. I will address this later under the specific sorts of frauds.

6.1.3.4 Audit and investigate

Audit processes should explicitly check for all of the issues identified in this book and, when they find them, the results had better be properly documented and reported to assure that responsibility is placed where it lies. In most cases involving frauds, detection comes from an audit or other detection process, and investigation is required in order to figure out what is happening, who is doing it, and ultimately to catch and prosecute them.

6.1.3.5 Adapt

A key to success in fraud defenses for corporations is the ability to adapt over time to the changing nature of frauds and to change the way they do business to eliminate the sorts of frauds that really hurt them. This adaptation leads some businesses to succeed where others fail. But it takes investment that many executives fail to appreciate until it is too late.

6.1.4 Specific methods for specific fraud classes

The fraud types identified earlier under corporate and financial frauds can be mitigated by many methods. I will outline some of the things that have worked for others here.

6.1.4.1 Time shifts

Time shifts are tricky for people using computer systems because most computer systems don't understand time but keep track of it rather well.

6.1.4.1.1 Currency windows

What is usually lacking is a process by which the date window surrounding the date of entry differentiates things that are current from things that are not. Anything that is entered into a computer that is not current should be questioned and independently reviewed. This is not just an indicator of fraud, but it is also a matter of business and process efficiency. When someone enters a payment three weeks late, it creates problems with customers and collection processes, and when someone enters a bill early, it creates the same problem. Anything pre-dated and anything post-dated by more than a few weeks should be reviewed. If this happens at a higher rate for some people than for others, it should signal suspicion and investigation.

6.1.4.1.2 Performance audits

Time shifts having to do with write-offs and other rates are generally dictated by law or regulation, but may just be a matter of poor expectations. One way or another, things like bonuses and other rewards that are related to performance over time windows should be arranged so that they are given but not paid until the numbers are proven to be correct in fact. For example, an end-of-quarter bonus or a bonus based on profitability should be subject to audit with high penalties for wrong numbers.

6.1.4.1.3 Align rewards properly

It is vital that rewards associated with behavior be aligned with the company's well being. People game the systems they work in to optimize their returns. If a company wants employees to do the right thing, they should build proper rewards and punishments for desired behaviors in proportion to their import to the company.

6.1.4.2 Cooked books

Cooking the books essentially always involves outright criminal activity. It is just lying in the simple sense of the word. Audits are the best way to detect most of these sorts of lies, and auditors should explicitly look for each of the scenarios described here as part of their periodic reviews. Anyone who cooks the books should be prosecuted and terminated immediately. Anyone who fails to take such action with regard to cooked books should be terminated, sued by the company, and investigated for possible criminal involvement in the fraud.

6.1.4.3 False valuations

False valuations are not easily detected when done in the small. A classic example of over-valued inventory is just plain hard to find, and the best estimates are rarely good to within less than a few percent. False valuations do have certain characteristics. One characteristic is that they tend to go in the same direction all the time, favorable to someone who stands to gain from them. So if errors in valuations are not statistically random, they may well be indicative of frauds. Another good practice is to track valuations from claims to realities at liquidation. When there are substantial differences, take recourse against those who did the valuations.

6.1.4.4 Manipulated goods

Once goods leave inventory, there is little that can be done about them being manipulated. So this means that inventory should not release items of substantial value. Someone typically has to write things off, but when they do so, there should always be a scrap value and the value should be tracked through the lifetime of the items until they are sold or certified as destroyed. Individuals are often placed in control of manipulated goods. By putting pairs of people on most delivery and pickup tasks involving scrap or other items, companies can reduce frauds to those involving collusion. By shifting partners and who is tasked with what, and taking statistics on results, frauds can often be detected. Errors in estimates of load sizes, for example, will tend to always be off in the same direction for frauds and be random for non-frauds. Frauds tend to skew performance indicators for those who commit them.

6.1.4.5 Off book

The problem with off-book actions is that there tend to be few if any records of what took place. The solution is to detect things going off book and get them back into the books.

6.1.4.5.1 Off-premise action reviews

Most off-book schemes that defeat these defenses involve things that never directly touch the company. Bribes and kickbacks are typically cash and never involve a company account at the target company. Most of these processes can be protected by having independent reviews at least on a statistical basis. For example, bids for goods or services should be reviewed by purchasing independent of the attempted purchase by an employee.

6.1.4.5.2 Thresholding and statistical reviews

Thresholds should be applied. For low value items and quantities, statistical reviews should be done, while for high valued items more stringent controls should be put in place. This way, higher consequences are more certainly mitigated while low-level frauds are caught over time through statistical methods. For high valued projects requiring special expertise, like buildings, plants, facilities, medical systems, or information technology issues, independent validation should be considered. The independent validation should be undertaken by someone who is not in any way involved with the project effort, perhaps working for the CEO, the board of directors, or the audit committee.

6.1.4.5.3 Skewed statistics reviews

Again, statistical comparisons of performance, price, and other similar indicators will be random for normal employees and skewed for people who either cannot estimate very well or are fraudsters.

6.1.4.6 Banking and credit manipulations

Most of these sorts of manipulations are detectable, when done in substantial quantity, by patterns associated with the particular scheme and statistical deviations skewed in one direction.

6.1.4.6.1 Fraud pattern detection systems

Companies like American Express and Visa have extensive fraud detection schemes to seek out specific patterns and, based on a real-time assessment of risk, decide whether to take additional

steps to determine if fraud is present. Purchase patterns of individuals are even used along with correlation of location to purchase, for card present transactions.

6.1.4.6.2 Kiting controls

For the bolder maneuvers, like credit card kiting, there are regulations in the contracts with credit card companies that indicate that you may not pay off one credit card with another. But those are ignored by fraudsters and most of the contracts are unreadable due to small print sizes and incomprehensible due to legalese, even for me, and I read contracts I sign thoroughly all the time. In addition, credit companies often check against credit bureaus that hold records on payment histories, income levels, and similar data for individuals and their family members. Typically, they try to limit the total available credit across all credit cards so that the total that an individual can ever take is limited by their financial situation over the medium term.

6.1.4.6.3 Personal privacy limits

Because many such frauds are relatively quick one-shot deals, long time frames are indicative of more stability, and trust builds with time. However, fraudsters are increasingly deciding to spend years of effort to generate hundreds of thousands of dollars of theft in each of scores of accounts. These big thefts are harder to detect, but can be detected by augmenting credit checks to include more and more personal data. These fraudsters, combined with the desire for credit by legitimate people, are the main driving forces in reducing personal privacy.

6.1.4.7 Fake companies

Any company that your business is doing business with should be checked out before you start working together. How long have they been in business? How does their credit check out? Who runs the company and what is their history?

6.1.4.7.1 Credit limits and background checks

Every company your company deals with should have credit limits that are reviewed by an independent credit group before credit is given to them. And the standards should be clear and never bypassed. Except of course that small businesses usually don't do

this very well and executives are often the targets of the scams and the ones that are authorized to bypass the credit requirements. Just say no to frauds by refusing to allow executives to break the rules without agreement by a group of other executives.

6.1.4.8 Trading places

The thing about trading places is that everything seems to add up after you are done. So audit processes have to be at a very detailed level in order to catch specific instances. Returns not properly weighed with excess converted, slush funds, checks for cash, and so forth are hard to detect automatically. While there is hope for doing statistics on individual performance and identifying individuals who seem to have consistent deviations in the same direction, this is hard to do, takes time, and produces no direct evidence.

6.1.4.8.1 Surveillance

Another approach is the surveillance of activities where these sorts of shrinkage happen. For example, surveillance cameras looking at cash registers in convenience stores and card tables in gambling establishments are reviewed based on performance indicators or at random. Experts detect the behaviors perpetrators are prosecuted. This works for activities carried out at specific locations, but is not effective for similar acts that are more mobile.

6.1.4.8.2 Strong internal controls

Various schemes like false invoices, double payments, and so forth can be largely eliminated by proper purchasing and payment controls. All purchases require approved purchase orders and can only be made from registered vendors. Purchased goods are not paid for until they are received and verified as to contents and quantity by the receiving department and placed into inventory. Payments only get made after approval by the purchaser of goods that are checked in by receiving. Payments are carried out by a group that is independent of purchasing. There are other similar rules involved in a proper system, but you get the idea.

6.1.4.8.3 Auditing

Under- and over-reporting and similar activities are also stopped by audit and random sample verifications. Once a fraud is detected, the employee needs to be terminated. Others in similar positions need to be warned of the consequences by the security awareness program. You do have a good security awareness program, don't you?

6.1.4.8.4 Independent reviews of write-offs

Write-offs and all of the things associated with write-offs and alteration of valuations are problematic and must be addressed by independent review of such activities. The various shifts involved in manipulating valuations almost always involve some estimate or an authorize individual making a judgment. It's only prudent to have those judgments checked out by the audit process.

6.1.4.8.5 Time delays for select actions

In order to facilitate this, there should also be built-in delays so that shifts cannot be turned into realities unless and until they are reviewed. For example, a 6 week delay on any write-off, for review and audit before approval, will cause great problems for most of these sorts of frauds, without having a significant effect on normal business operations.

6.1.4.8.6 Check verification technologies

Check bleaching and other alterations associated with checks can be largely eliminated by using the systems that transmit all of the information on checks to the bank. These systems require the bank to verify that the check is as indicated before clearing it. This has largely eliminated check frauds for those who use it, but at a cost.

6.1.4.9 Load shifting

All of the shifting of personal expenses to company accounts was classically handled by requiring original receipts for everything, but that is no longer effective because of the use of computers for most such transactions. As a result, I can print multiple copies and make digital alterations that are, in practice, undetectable by inspection.

6.1.4.9.1 Company credit cards

One solution lies in company credit cards. All reimbursed expenses over a certain level must be charged to the company credit card or done with a purchase order that generates a check. Then the credit card receipts can be verified against employee reimbursement invoices. This should be required for all meals, transportation other than taxicabs (which are often cash-only or very inconvenient for credit cards), communications charges (which should be using cell phones or office phones that are again auditable), and almost anything else I can think of. The credit cards are of course the personal responsibility of the employee even though they are in the company's name, and the company will only reimburse purchases made on the company card. You can even arrange that they have daily, weekly, and monthly thresholds for credit limits.

6.1.4.10 Employee frauds

All employees and other workers should be checked out with some sort of background process before being allowed to work.

6.1.4.10.1 Background checks and audits

At a minimum this should include contacting each of their references personally and discussing the potential worker with them, checking each job they have claimed to have, checking their educational background with the schools, and verifying that they have no criminal records. These checks should not use the information provided by the candidate for contact, but rather should be done by using the telephone directory or other similar public method to find and contact them. This process should be done by the HR department and audit should verify that this is done for each case.

6.1.4.10.2 Qualification checks

Specific qualifications for each job should be provided and unqualified workers should not be permitted even if they are the boss's daughter. At least she can work in something she is qualified to do.

6.1.4.10.3 Auditing work hours

Time card fraud should be checked by audit processes and employee reviews should indicate what they have accomplished so it can be verified by audit.

6.1.4.10.4 Manager review and investigation of legal claims

Workers compensation claims that are considered fraudulent by the manager or other workers should be reported to officials and, if necessary, private detectives should be used to determine if these are fraudulent. Background checks should clearly indicate prior history of such claims and if prior history is not reported from prior employers but found in present employees, a law suit should be undertaken against the former employer to get records and, if they indicate a history of such claims, the suits should be extended to cover damages from their failure to notify.

6.1.4.10.5 Check out your employer before accepting

Potential employees should check out the companies they intend to work for before providing all of the information requested on an employment form. If you can't determine enough about the employer to be sure you want to work for them, you need to seek a different job. They should be easy to find since most companies want people to know about them. You can also look up their customers and business history to get an idea of whether they are worth working for.

6.1.4.11 Floats

Floats are especially tricky because the time to process things is dictated by the process used. If you don't, at some point, trust that the transaction is completed, you are always waiting to do business, which means your capital is not being used as well as it can be. Large companies with large cash accounts transfer them to overseas accounts for the 16 hours of interest every night, and when you have a billion dollars in your cash account, that can be considerable - on the order of 2/3 of 10% of a billion dollars per year, or $66 million dollars per year.

6.1.4.11.1 Calculate and manage risks

So the problem lies in crediting the accounts but not granting access to the money. Banks are getting good at this so these sorts of kiting schemes tend to be problematic in normal banking transactions. But for things like credit cards, this can get nasty fast. The problem is that the whole credit system is based on a trust relationship that basically determines trust in individuals based on history. Companies that build up more of these customers and retain adequate rations of legitimate customers to frauds win more of the market. So a risk management calculation is undertaken to figure out on what basis credit can be granted so as to increase volume while keeping risks within thresholds. Increased interest has to be used when risks are higher, but when people pay on time, there is no interest today.

6.1.4.11.2 Faster checks and shorter floats

The best outs include faster and less expensive automated credit checks with credit bureaus becoming real-time information sources and taking on liability for accuracy, integration of things like homes equity and for sale situations with credit lines so the credit can be recovered from equity at sale, and other similar methods. But this is not integrated well today, so as an alternative, after such frauds start to appear, common patterns are generated and used as a basis for analysis. The fraud squad at the credit card companies keeps eternally busy seeking out new methods to detect frauds before they get burned, just as the fraudsters eternally seek out new ways to exploit the remaining weaknesses.

6.2 Government and law enforcement

Governments have to deal with everything from minor frauds to intelligence operations. As a result, they have the full spectrum of requirements and need to deal with them with different methods.

6.2.1 Segmented approach

So they use the business and financial approach for monetary issues, the OPSEC approach for intelligence operations, the law enforcement approach for law enforcement issues, and the personal perspective for its workers and citizens.

6.2.2 Law enforcement approach

The law enforcement perspective is pretty much embedded in everything that law enforcement does. Officer safety is embedded in police training from the first day on the job, and because many police officers deal with frauds every day, they are well aware of the techniques and pretty much take them in stride.

6.2.3 OPSEC

Law enforcement used operations security when they do covert operations and they take officer safety seriously. Police work with partners in essentially all operations, no matter what the television shows may say about them, and they get lied to so often that they operate on the basis that everything they haven't checked out can be a lie or the truth. Which is to say, they check things out, follow

procedures, document what they do, and follow rules that largely keep them out of trouble. Those that don't, learn the hard way.

6.3 The personal perspective

Individuals, you, me, and most of the other people we know are the ones that get stuck with most of the frauds. We don't have organizations behind us teaching us about personal safety, training us in how to defeat fraudsters, or telling us about the newest techniques that the bad folks are using. We aren't always on the lookout for lies and deceit, we are trying to make friends, and we don't have a lot of secrets to keep that foreign governments would want to pay for or trick us in order to get. Most of us are just trying to make our way in the world, have some fun, live well, eat well, and go about our business.

What we do have is the every day frauds and scams. People that try to take advantage of us by telephone, email, Web sites, mail order catalogs, knocking on our door, meeting us in a mall, or accosting us on the street. So what do we do about it?

6.3.1 Three easy steps to reducing susceptibility

There are three easy steps to take to reduce your susceptibility to frauds. If you have read the first 182 pages of this book or so, you have largely completed the first step.

6.3.1.1 Step 1: Know thyself

The first step to personal fraud protection is to understand who you are and what you are. People that take advantage of other people largely do it by projecting an image of their victim that is not very realistic, but meets the target's vision of themselves or their lives in their dreams. Do you want to be thin? Do you want to eat well? Do you want to have fun? Do you want whatever it is that you want? Then you can get it by giving your money to me!

6.3.1.1.1 I'm old, overweight, and married

I am overweight. I know it. I try to lose weight and have tried for many years. I know what will work and what will not because I have succeeded by doing it and failed by not doing it. The way I lose weight is by eating less. That's it. If a gorgeous 22 year old girl comes up to me when I am on a trip, no matter how exhausted I

am, I know that she is not there because I am her dream of a lover come true. If I am, sorry, I'm already married.

6.3.1.1.2 I am not the Rolex type

I am also not the person that people from Africa come to as their trusted partner who has such high integrity that I will hold their illegally obtained $50 million while they skip the country. I know that I cannot afford a Rolex, and if someone tells me that I can do it by selling it at a low low price, I know it must be a lie.

6.3.1.1.3 I miss golden opportunities – on purpose

Will I miss some golden opportunity some day? Sure I might, but I will also miss all of the rotten opportunities to get ripped off by uncaring malicious people who live by taking advantage of the good nature of others. Know yourself and don't let people that you don't know persuade you that you are somehow different than what you really are. Sure, make fast friends when you encounter them, but don't trust them with everything you have until they have earned your trust.

6.3.1.1.4 Think before you act

A friend in need is a friend indeed. So ask yourself what deeds they have done to make you think that you should trust them with your wallet, your checkbook, your briefcase, or your car. If you have known them for years and they need to borrow your car, feel free. But if you never met them and they claim to be acting on behalf of your friend or neighbor, help out by contacting others you know and coming to help as a group.

6.3.1.2 Step 2: The golden rule - in reverse

Treat others as you would be treated and you will be doing the world a favor. But what's the golden rule in reverse? That's easy. Expect to be treated the way you expect to treat others - the way you want to be treated. If people don't treat you that way, you need to straighten them out and tell them to treat you right.

6.3.1.2.1 Would you do it?

Do you expect that someone who you never met will give you a lot of money and have you take it to the bank for them? Is that what you would do in a similar situation? If not, don't go along with it. Try taking them to the bank with you and don't take their money for helping them. Expect to do good without being rewarded and if you get rewarded, that's fine too, but don't expect it and don't take more than what is reasonable. Don't expect that you will get something for nothing any more than you would expect to give someone something for nothing. Put yourself in their shoes and think about what you would do. If what they are doing does not make sense to you, don't go along with it.

6.3.1.2.2 Hang up on telephone solicitors

I just got a phone call. The ringer rang and I picked it up and said hello. There was a delay as the computer on the other side figured out that I was a human being so they could start their automated playback. I hung up before I heard the pitch. I expect that when someone calls me they call me personally to talk to me because they know me or have heard of me. I expect that they are calling me personally. If they are not, I don't want to talk to them and I think it is wrong for them to do so. I don't call people who I don't know trying to convince them to send me money and I expect that they should honor my privacy as well.

6.3.1.2.3 Demand fair treatment

To quote one of the players in "*Oklahoma*", a wonderful musical if you haven't seen it, "*I don't think I'm better than anybody else, but I'll be damned if I ain't just as good.*" Expect to be treated right in your life, demand it, and take nothing less.

6.3.1.3 Step 3: You can be nice and also be reasonable

Just because you don't let yourself get ripped off doesn't mean you have to be nasty to other people. You can politely say no and walk on when the fraudster tries to approach you on the street. If you live in New York, you probably walk right by, ignoring people. But most people in smaller towns say hello to people they pass in the street. You can still say hello to strangers without getting ripped off.

6.3.1.3.1 Say no politely – buy flowers instead

Just because you are made an offer that seems too good to be true, doesn't mean that it is not true. The offer that seems to good to be true might be true, but it probably isn't. You can say no politely and know that while you may have missed a golden opportunity to get in on the bottom level of the greatest money making offer since the beginning of time, you have also saved enough money in doing so to buy your significant other flowers.

6.3.2 Expect that you will not always win, but try to

Will I end up donating to causes I think are good that turn out to be not so good? Sure I will. I want to help save dying children around the world by supporting vaccine programs and I want to help the Red Cross help natural disaster victims. So every once in a while I will get duped, but not too often, and not for much money, because I know that the right way to do it is by taking the time to look at what I am doing and do it the right way. And now, so do you.

6.3.3 When in doubt check it out

I like that saying. If you aren't sure, try to use alternative means to verify that the thing you want to do is real. If you get an opportunity to donate to an organization you think is doing good, check them out. Look them up in the phone book and call their headquarters. Make sure that the person you are dealing with is part of the organization and find out the way they normally take donations. Those dying children will be saved more efficiently if you take the time to get the money to them and not a fraudster.

6.4 Countering Internet scams

Nancy Reagan had it right here. Just say "No". You can pretty much bet that 99% of all the emails you get from strangers over the

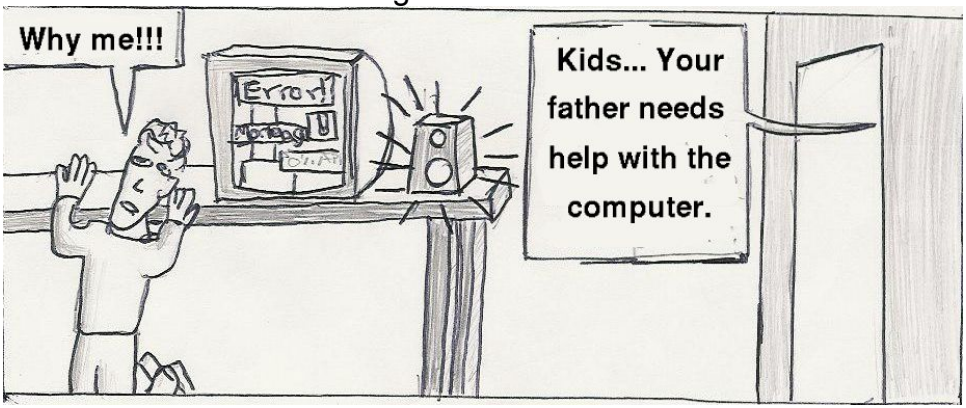
Internet are frauds. Just say no. Don't read them, don't check them out, don't try to investigate, don't click on the pretty girl's smile, don't watch the movie, don't download the special application you need to see the movie. Just say no and avoid the sleazy side of the Internet.

6.4.1 I can't help myself!

I hear your plea. You just have to see that new Internet whistle collection and they won't let you in unless you download the special module from stealmeblind.com. So what do you do?

6.4.2 50 Ways to Protect Your Assets

CyberCops are particularly vulnerable to exploitation when they are doing investigations on the Internet. To help them, and others who want to be safer when cruising the Internet, Kevin Manson and I provide this list of the 50 ways to protect your information assets when cruising the Internet. Ask your kids for help if you don't know how to do the technical things.



Oh yes. I promised to tell you the reason for using 50. In the 1970s Paul Simon wrote a song called "50 ways to leave your lover" that was very popular. So one day I was working on writing up a non-technical article on security and I decided to title it "50 Ways to Attack your World Wide Web Systems". It was my most popular article of all time. So I started a series of these articles and folks read them and liked them a lot more than my other work. So I stuck with it.

6.4.2.1 System configuration

System configuration must be done properly to have a modicum of security. Here are some configuration issues you should address:

6.4.2.1.1 Use removable media

Use removable media on Internet-connected computers. With removable media, you can put in the Internet disk when you are using the Internet, and replace it with the “secure” media when doing your work. It means that the bad actors can't get to your confidential information when you're on the net and your critical information can't get messed up by a virus or Trojan horse coming in from off the Internet.

6.4.2.1.2 Turn off "sharing"

Turn off "sharing" on NT and Windows boxes. Sharing of files lets Internet users access your disk from anywhere in the world. With sharing turned off, they have to break in to get at your system.

6.4.2.1.3 Turn off ActiveX

Turn off Active X, Java, and Javascript. These capabilities help you make pretty pictures, but they also allow the bad actors of the Internet to enter your system and do with it what they will.

6.4.2.1.4 Use properly configured bad content detection

Use properly configured software to assist in detecting viruses and malicious code. If your virus scanner can handle it, have it check for macro viruses in real-time.

6.4.2.1.5 Keep a clean copy

Keep clean and current copy of system start-up and restore software handy. This way you can recreate a working system in a flash and avoid long downtime when you do things like upgrading software versions over the Web and finding out that your system is locked up.

6.4.2.1.6 Backup, backup, backup!

Yes - keep three copies just in case.

6.4.2.1.7 Keep software patched

Keep your software up to date with security-related changes. For example, without the latest version of your browser or email program, you may find that when you go to read email - even

before you open up any of the messages, your system has been taken over by a remote attacker.

6.4.2.1.8 Turn off unused services

Turn off unnecessary Internet service ports. In general, if you don't know why your system uses a service, you should not have that service turned on. Every service is a potential vulnerability.

6.4.2.1.9 Scan yourself

Use a scanning tool to test which ports are turned on. Never trust the menu-based configuration tool to tell you this because many of these tools have errors, some of which have opened systems up to remote exploitation even though users who “did the right thing”.

6.4.2.1.10 When in doubt, print it out

If it's really important to document, print it out. Remember that paper trails are a lot easier to use and authenticate in court than electronic media.

6.4.2.2 Passwords

Passwords have been a security issue for a long time, and most people still don't know how to use them safely. You need to know how to create and use passwords that are properly crafted to the need.

6.4.2.2.1 Use unique passwords

If you have anything important on a remote site, use unique passwords for each online service and site. Otherwise, someone breaking into or watching one service could use your password in other services.

6.4.2.2.2 Don't share passwords for important sites

If you are going to use the same password for multiple sites, make sure they are not important sites. For example, whenever I get a password for a remote site that is not important, I try for user ID guest, password guest. This may weaken their security, but if they allow it, their security is already very weak, and it is easy for me to remember and doesn't give anything away about me or the kinds of passwords I use for important systems.

6.4.2.2.3 Remember your passwords may be sniffed

If you are accessing remote services on the Internet, remember the passwords can be easily recorded as they flow through the Internet (sniffed). Try to avoid using passwords for Internet-based access.

6.4.2.2.4 Never use your local password

Never use a password over the Internet that's the same password you use on your local systems. That might allow someone from the Internet to break into your systems.

6.4.2.2.5 Use one-time passwords

Try to get and use one-time authentications of some sort. These are relatively inexpensive (Deception Toolkit at all.net has one for free) and very effective.

6.4.2.2.6 Augment authentication

When possible, augment passwords with some other form of authentication. For example, use TCP wrappers or some other similar tool to limit the remote addresses that can access a critical system, or use a separate channel to enable remote login.

6.4.2.2.7 Don't change passwords over the Internet

When you have to change your password, don't do it over the Internet. It is easily sniffed. If at all possible, do it from the computer with the password on it.

6.4.2.2.8 Change passwords periodically?

Changing your password regularly is not prudent for all systems or situations. Consider the real benefit and harm associated with this activity before doing it haphazardly.

6.4.2.2.9 Use hard-to-guess passwords

Some passwords are harder to guess than others. Use the harder to guess ones. Examples of easily guessed passwords include (1) your name, user name, or other available information associated with you, (2) any word or pair of words in any language, (3) QWERTY or similar keyboard patterns (but not all keyboard patterns are easy to guess), (4) passwords of less than 7 keystrokes, and (5) passwords with only numbers, only letters, or the same character repeated.

6.4.2.2.10 Don't let others use your accounts

Don't let other folks use your user name and password and don't tell anyone your password. This lets them fake being you and you are likely to be the one who gets in trouble if they do something wrong. No legitimate person responsible for security or systems maintenance needs to know your password, and there are almost no exceptions to this rule. (Check your organization's policies in this regard.)

6.4.2.3 Don't trust downloaded software

It may contain Trojan Horses that are potentially devastating in their effect. Examples of how this has been exploited in the past include but are by no means limited to (1) causing your system to dial out to a 900 number for Internet service, (2) stealing your online information, (3) corrupting or destroying information on your system, (4) turning the computer into a jumping off point to attack other systems, and (5) placing a Trojan horse in your system to permit remote reentry and exploitation at a later date.

6.4.2.3.1 Turn off "autoinstall"

Turn off "autoinstall" features. Autoinstall allows remote sites to automatically change what your system does by installing their software.

6.4.2.3.2 Know what's supposed to run

Become familiar with the "processes" that are authorized to run on your machine and how to check on them. Check them periodically and whenever you suspect or observe abnormal system behavior.

6.4.2.3.3 Watch for email attachments

More viruses spread today through email attachments. Be careful how you use email attachments and who you accept them from. When I don't know and trust the person sending me an email attachment, I either ask them to send it in plain text format and not as an attachment, ask them to FAX it to me, or copy it off of my system onto a non-networked system and read it there.

6.4.2.3.4 Disable Word macros

Don't use Word attachments without Word configured to disable all macros before execution. Otherwise, you can easily be attacked by an email.

6.4.2.3.5 Don't trust spreadsheets

Don't trust excel spreadsheets. They not only give wrong answers, but they can contain "CALL" macros to attack your system and there is no mechanism to detect or prevent this available today.

6.4.2.3.6 Don't trust their programs

Don't trust any program - whether it comes in source or in executable format - without seriously considering the potential implications of its installation and use. Many programs innocently do things that weaken your security, and in lots of cases they allow remote exploits against your system.

6.4.2.3.7 Data is sometimes program

Just because it isn't called a program doesn't mean it isn't a program. Most information you get is just plain “data”, but some of it is not, and it is hard to tell the difference unless you are a real expert. But you can't stop using computers just because you don't trust them, because they are required in order to get the work done. Just understand that you can get hurt and prepare to suffer the consequences.

6.4.2.4 Keep up to date

Keep up to date on the information security issues that might effect your system.

6.4.2.4.1 Get on the right lists

Subscribe to computer security lists such as NT Bugtraq, NTSecurity Digest, etc. Read about the newest attacks and update your system to mitigate them.

6.4.2.4.2 Patch your system

Keep your system up to date with the newest security patches for the software you use to cruise the Internet.

6.4.2.4.3 Get systematic with your system

Realize that computer security requires a systematic, not a piecemeal, strategy to be effective. 50 ways are only the beginning.

6.4.2.4.4 Think like an attacker

How would you attack yourself? You might read some of the hacker FAQs on the Internet or try an automated attack and defense game to get a sense of what people might try to do to you and how. You

might want to see how attackers think by exploring one of the games on the all.net web site.

6.4.2.4.5 Think broadly about security

Don't forget other communications channels that may be vulnerable, such as voicemail.

6.4.2.4.6 Ask others for help

Ask others who are competent to review or audit your security practices. Your children can probably help a lot, and they probably also know friends who are even more knowledgeable.

6.4.2.4.7 Paper is pretty good

Don't forget that critical data may be far more resilient to degradation or corruption when placed on paper than on magnetic or optical media.

6.4.2.5 Use security technology wisely

Use available security technology to your advantage, but don't just buy anything "security".

6.4.2.5.1 Anonymize yourself

Become familiar with methods of anonymizing your online sessions like “Onion routing”, “ZKS”, “anonymizer”, and "mixmaster" type anonymous remailers. Remember that the bad guys use them (and may run them) too, and don't trust them alone for anything important.

6.4.2.5.2 Encrypt communications

Begin to routinely encrypt any important communications and encourage (and assist) others in doing so.

6.4.2.5.3 Check before send

Whenever you encrypt, always try to view encrypted files before sending them. Encryption systems sometimes don't do what they say they do.

6.4.2.5.4 Use public key cryptography

Generate a public/private key pair and let others know how they may obtain it.

6.4.2.5.5 Sign your emails

Digitally sign e-mail where authenticated identity or unmodified content is important.

6.4.2.5.6 Sign important files

Digitally sign important files and documents that you believe others may wish to rely on as to their integrity and authenticity.

6.4.2.6 Use uncommon sense

Common sense is not that common. So try to get sensible about computers to be safe on the Internet.

6.4.2.6.1 Don't ask for trouble

Don't visit the bad-guys' sites. Remember that they can see you when you can see them.

6.4.2.6.2 Stay away from the seedy side

Don't go cruising through the seedy side of the Internet unless you are ready for the seedy side to go cruising through you.

6.4.2.6.3 Don't respond

Don't respond to email from lists you haven't signed up to, especially if they tell you that you can “unsignup” by sending them mail. This is how they confirm your email address as valid.

6.4.2.6.4 Postings bring spam

Never post to public bulletin boards or mailing lists unless you want to get anonymous email from lots of places. That's one of the major ways they get email addresses.

6.4.2.6.5 Don't go to pornography sites

Don't visit it. You are likely to get a great deal of follow-up from a very broad range of sources you don't want to deal with.

6.4.2.6.6 In the computer is on the net

The information you place in your Web browser (like your name, address, organization name, and so forth) are available to the Web sites you visit. Don't place information there unless you want it given to every site you visit.

6.4.2.6.7 They share your data

Every site you ever visited may be revealed to any site you visit.

6.4.2.6.8 Your system remembers

Your system keeps records on most places you visit. Many of these records can be remotely accessed, and local access grants a lot of fine details of when what took place.

6.4.2.6.9 If they get in they get your keys

If the bad guys get into your system, they can get all of your cryptographic keys, your passwords, and anything else you have placed on your system.

6.4.2.6.10 If they get in, they will exploit you

If the bad guys get into your system, they can use your system to get into other systems it can connect to. This often includes other computers inside your firewall.

6.4.3 Countering email frauds

The best countermeasure to email frauds is to delete all such emails as soon as you get them. How do you know that's what it is? If you get a message from someone you don't know, and it is not a personal message really to you, delete it. If it seems like a message to you personally and it is not about what you do every day, delete it.

6.4.4 Countering news group frauds

News groups frauds appear as spam. Delete those postings and get off of lists that have a lot of them.

6.4.5 Countering chat room frauds

Chat room frauds are tougher. If you can detect it is a fraud, you should tell everyone on the list that you think that and if you know how to set up an autoresponder, create an automatic response to every use of that identity that flags the sender as a fraud to the whole list every time they send a message.

Never trust that someone you encounter in a chat room is anything like what they appear to be. They are likely as not just plain lying. They may be playing with your affections or trying to steal from you, or they may be legitimate, but not very often. Chat rooms involving total strangers are never a good idea to get into. The local bar or bowling alley is probably a better place to meet people.

6.4.6 Countering Trojan horses

Trojan horses come from loading software into your computer from the Internet. It may come in email as an attachment, so turn this feature to the mode where attachments are not automatically opened when you read the email. Don't download computer programs from the Internet, and follow the 50 Ways.

6.4.7 Countering Internet child exploitation

For your kids, chat rooms should not be allowed. I tell my kids that they can chat with people that they already know from school using a chat client, but only one-on-one and not in a chat room. I explain it to them and they seem to understand and listen.

6.4.7.1 No personal information on the Internet

I tell my kids not to put any personal information in a chat room and never ever arrange to meet someone who you have only encountered in a chat room. For adults, some of my kids are now adults, I tell them to only meet in a very public place with a lot of your long-time friends present.

6.4.7.2 Watch openly

I look at the chats my kids are in. I don't sneak in, I just walk up to the screen and look with them sitting there. If they turn off the screen or try to close a window as I walk up, I tell them that I have to be able to look at what they are doing for their safety and that if they are going to use the Internet they have to follow these rules.

6.4.7.3 Be clear and unapologetic

I try to mix clear explanations of what I am looking for with my interactions with my kids, and try to make it as clear as possible that they should not trust people or things from the Internet unless they already knew and trusted them before. I try to make it clear that it's about their safety and well being and not about me wanting to stick my nose into their business. And I make it crystal clear that until the age of 18, I am legally and morally responsible for their well being and that this is the only way I know that I can carry out my responsibility without trying to lie to them or conceal my concerns or my actions. They have taken it well and, despite the occasional dispute, there is peace and love and safety.

6.5 Recognizing and defeating propaganda

The first best step to recognizing propaganda is to assume that anything a government tells you about a war they are trying to promote is propaganda.

6.5.1 People are not demons

When it comes to hating someone, resist the temptation. When it comes to calling someone else less than human, don't buy it. People are people, not sub-beings, not short catchy name things like *Glags* or *Slats.*

6.5.2 Everyone can be and often is wrong

If "*everyone*" says so, ask someone else who doesn't. If the media is hyping it, look at the alternative media. If a movie promotes it, there is another side to it. Do your own research, even though it's easier not to think.

6.5.3 Endorsements are easy to get

I got a letter telling me that I could get Alexander Haig, one time US Secretary of Defense, to endorse my company on a video that they would make for only $16,000. Rest assured that I don't know Alexander at all and he knows nothing of my products or services. That's how hard it is to get an endorsement.

6.5.4 Branding is for cattle, don't be cowed

When you see clever sayings, or when political systems are linked to good and evil, or when there is an "*ism*" involved, be leery. When the name of the war changes, you know they are seeking the brand you will most like. When they ask you to believe in something or be loyal to something, think hard about where your real loyalty lies. Are you loyal to the President or the country? They are not the same thing.

6.5.5 If they all say it, it is a script

A dead giveaway is when everybody in the government who speaks on an issue uses exactly the same words or phrases. This means they are being coached to tow the party line and it means that advertisement is in play, not honest individual opinions. If you are listening to a news channel and the reporter says the same thing as their opinion, they are part of the government propaganda

campaign. Change the channel and complain to the station and your congressional representative. They are your airwaves!

6.5.6 Overcome the big lie

When people in authority, leaders, highly respected authors, and news people on the channel of your choice keep saying the same thing day after day and week after week, don't buy it. The longer they say it, the more likely it is a lie, because if it was true, they wouldn't have to keep repeating it to make it seem true. If the so-called good guy, the insider portrayed as an internal opponent, tows the party line, be especially careful. Either it is the big lie or the independent has been lied to and has now become a believer.

6.5.7 Single speak

When you hear doublespeak, split it up. Take it in its parts and see if they are really linked. When the sentence seems to make sense but you don't really understand it, it is likely not because you are not smart enough. It is more likely that you are smart enough to know that it is doublespeak but that until you understood its nature, you didn't know it. Now that sounded like doublespeak.

6.5.8 Bring voice to the opposition

When the opposition is being silenced or when everyone you talk to seems to agree, it's time to voice the loyal opposition. You don't even have to believe it yourself, and you can portray it as what you heard or what you were thinking, but give voice to the opposition. Seek it out, evaluate it, think through it, and make your own decision. Help others see it, even if you don't agree with it, so they can make up their minds as well.

6.5.9 How can you be sure?

If you appear to be against it and they slam you, you know they are lying to you. Just as the fraudsters try to gain compliance, so do the propagandists. You can tell they are not genuine if they don't respect your right to have a different view.

6.6 De-frauding your life

OK. That was a pretty bad play on words. But the point is a valid one. Living a life without fraud involves taking your time and thinking through what you do. If you are out for a quick buck, you

are easier to defraud. If you are always looking to get rich quick, others will get rich quick off of you.

6.6.1 Don't be a target

I'm not telling you not to be ambitious. I am telling you that working hard and working smart both bring the things that you need and desire in life, especially in the free countries of the world, especially in the days we live in. If you are trying to find an easy way to get ahead or if you are trying to figure out how to take advantage of others, you are more likely to be the target of frauds. The reason is simple. The very behaviors that you are exhibiting are the ones that make it easy to defraud you.

6.6.2 Think about what you see

Think through it. Most frauds are either exactly like or very similar to the ones described here. If you read this book and take it to heart, you will understand what to look for and be able to spot most frauds a mile away. You don't have to be paranoid to be alert to what is around you. Think about what you see as you walk through the world, and try to make sense of it. You will avoid most frauds before they get close to you.

6.6.3 Stay away from the seedy side

You can't defeat frauds when you are drunk or stoned and all alone in the street at night. You can't do it when you are in the hectic part of town where all the wild times are. I'm not telling you not to go there or not to get drunk. That would be a different book. Go ahead. If that's what you enjoy, enjoy it. But expect that you will be targeted and be prepared. Expect to spend or lose what's in your pockets. Go with friends and stay together - it's safer and more fun. If you're going there to find a friend, be prepared and understand that just as you could find your best friend for life, you could also find your worst enemy.

6.6.4 Limit your losses

There are lots of ways to limit your losses - just like the big guys do. You just have to pay attention to it. Here are some chunks of advice for losing less.

6.6.4.1 You can't lose it if you don't have it

Sort of. If it isn't with you, the fraudster has to have you go get it. That means that you have time to think about it. When you go through life, don't carry big wads of cash around with you. Don't carry more than you can afford to lose.

6.6.4.2 Credit not debit

You can only lose what you have with you - sort of. I use credit cards and they have limits on them. US law limits my personal losses to $50 per credit card if I report them as stolen or report frauds when I see them. Debit cards allow a fraudster to take all the money you have in the bank right away. And you cannot get it back. End of story. Insist on a credit card, not a debit card.

6.6.4.3 Don't take it with you

If you are headed out to somewhere where you are more likely to get defrauded than you are at home, only bring things along that you can afford to lose. Don't bring your gold ring or your diamond neckless into a crowded party in the red light district unless you want to have it stolen. If you want to have it stolen for the insurance money, don't expect to see the money until the investigator finds out why you brought it there after I warned you not to.

6.6.4.4 Set boundaries

When you invite people into your home, you are showing them what they can take. Most people you meet and invite home are probably very nice people, but some may not be. So when you first meet them, if you invite them home, anticipate the possibility that they will want to do you harm or not really be your good friends.

As an alternative, set boundaries. If they are in your home, they should not be allowed to go just anywhere unsupervised. Perhaps your bed rooms or your home office are out of bounds to them. Maybe you keep your financial records in a file cabinet, why are they looking through it? People need to set boundaries associated with their comfort levels and friends respect friends' boundaries.

These boundaries also apply to your personal space and physicality. People within your personal space have a tendency to

be able to take without asking. Pick pockets and other sorts of thieves use bumping techniques to allow them to take without you noticing it. Fraudsters do the same thing in your mental space.

6.7 Specific defenses for specific fraud types

For each of the types of frauds described so long ago in the front of the book, there are specific identifiers and specific defenses. While the generic defenses work well across the board, these specific defenses get you out and away, hopefully without a scratch.

6.7.1 Fake paper

Fake paper frauds generally involve a few things in common. Paper that is not real or switched, you bring money to the table, and they get away from you before you figure it out and get your money back. So a few simple rules will help save the day.

6.7.1.1 Check the paper first, last, and between

When someone hands you a bill of goods, read the bill. Review all contracts thoroughly by actually reading them and don't sign them if you don't understand them and really agree. Get professional help if it is valuable, and if it is not, don't do the transaction. When you are signing the front copy, look at all the copies to make sure they match. Read both the front and back. It only takes a second to check. Check the paper before you sign, and after you finish.

6.7.1.2 Leave your cash in the bank

If there is cash involved, don't do it. There are almost no transactions that require cash anymore. Those that do are highly structured and unless you participate in such things for a living, avoid them. Car auctions are in cash, but unless you are a dealer they won't even let you in. Bankruptcy auctions are often in cash and sponsored by the court. But they are sponsored by the court and you can check the court to get the details.

6.7.1.3 Get verified information on them

Check the official records to make sure they are real and to get the right information. When you deal with someone, find out about them. If you are doing a deal for a few tens of dollars and you can afford to lose it, sure, go ahead. But if the money is substantial to you and the transaction is important, take the time to research it.

6.7.1.4 Short time limits are usually lies

Most time pressure is designed to get you to act foolishly. Take your time. You may lose a few percent on a deal here and there, but if you rush into it, you can lose a whole lot more. Big decisions should not be rushed and if they are trying to rush you they are likely frauds or pushy salespeople. Deny them the sale and go with people you are comfortable with.

6.7.2 Fake stuff

The fake stuff frauds generally involve showing you the goods, or at least a picture of them and some attestation as to their value and authenticity.

6.7.2.1 Try not to get that far

Unless you were looking for whatever they are trying to sell you before you met them, assume that they are frauds and move along. It's just smart shopping not to buy things you didn't want before you went to the store. If you decide you want it later, you can go to any store and buy it. If you can't, it's probably a fake anyway.

6.7.2.1.1 When in doubt, check it out

If there is any doubt, and remember, this is about something you were seeking out, engage an expert to help you tell the difference between the real stuff and the fake stuff. In many cases, experts are available for little or no money for simple questions. Go to your local University and ask someone in the geology department about recent gold strikes in California. They will help you find out there have been no real ones but several fakes. One technique I use is to go to the Internet and find competitors. I call them and find out what the market is like, what I get, what it costs, and how it works. I ask each of them about the others and comparison shop. I usually get the better company for a better price and better understand what I am doing in the end.

6.7.2.2 If you aren't an expert, don't trust theirs

Any time the other side brings an expert, don't trust them. If they just happen to have an expert handy, run away as fast as you can! If you need an expert to tell the difference, get your own from a trustworthy source. Call a professor, they need the consulting work.

6.7.2.3 Randomness isn't

If something really lucky happens, be highly suspicious of it. Seemingly random events in the presence of a fraudster are almost always seemingly only. If nothing else, take your luck as a sign and walk away with your winnings, but never open your wallet.

6.7.3 Looks like it

Most looks-like-it frauds involve the belief of the target that it makes sense because it looks reasonable. Most people don't want “more important” people to be mad at them and avoid confrontation. They can be shy, passive, or tired. As a result, they fail to inquire.

6.7.3.1 Question everything new

Why does it make sense that someone you never saw would be here to audit the cash register? Because you have never seen anyone do it before! If you bought that, you are going to lose to looks-like-it for sure. If it's new, you should question it.

6.7.3.2 Trust but verify

Check it out with the boss. This works recursively, so the boss checks with their boss, who checks with theirs, and when it reaches the biggest boss of all and they don't know about it, you are a hero. Otherwise you are a conscientious employee making sure to protect the well being of the company. All the better.

6.7.3.3 Be really friendly and helpful

Really helpful is even better. In fact, be so helpful that you follow them around every step of the way and watch what they do. Ask for their name and all about them. Introduce them to others. Ask to have your picture taken with them. Introduce them to the local police. But don't help them to do things you don't know they are allowed to do. Instead, help them get in touch with the person who is authorized to authorize it.

6.7.3.4 Don't judge a book by its cover

Just because I don't look like a bank examiner doesn't mean I am not one. After all, what exactly do they look like anyway? The UPS pickup person usually has a UPS truck right behind them. Just because I look old doesn't mean I am not a fraud. Fraudsters come in all shapes and sizes, just like regular folks.

6.7.4 Much for little

Much for little, or something for nothing, really don't exist very often. And when they do, they are usually part of some deal you don't want in on unless you set it up.

6.7.4.1 Did you really think so?

If you are one of those people who thinks that there really is a Santa Claus and that the government is here to help you, then you probably really do believe that you can have this boat for free, and all you have to do is take over the payments. It could happen! But even if you are not skeptical, just note that this is an unusually good deal.

6.7.4.2 How little for how much?

So just how good a deal is it? Do I get a ten million dollar lottery prize just for sending you $10 in cash? That's a million to one! It's too good. Suppose you put up the $10 and I will give you $10,000 of it for helping me out. After all, I can afford it. It's only a few weeks interest on the $10 Million you will be sending me. The better the deal, the more likely it is a fraud. But suppose it looks legitimate and I am willing to bite...

6.7.4.3 Is it a one-time offer?

What a stupid question. Of course it is. Buy it next time they offer.

6.7.4.4 Only available right now?

Can I do it tomorrow? No! It's a fraud.

6.7.4.5 Only for me?

I am the only person in the world who is this lucky? Fraud!

6.7.5 Relationships

This is the hardest one of all. Most people looking for relationships are lonely. Most people trust the people they are in a relationship with, and by reference trust those they trust. I'm not going to tell you not to trust those you are in a relationship with. But on the other hand...

6.7.5.1 How long have you known them?

Most relationship frauds not involving governments are designed to get closely involved in a few days or weeks. So for the most part if

you have known someone for a long time and are starting to get more deeply involved, it is unlikely to be a relationship fraud. Having said that, love at first sight is a fairly common phenomena.

6.7.5.2 Are they playing with your emotions?

If you look at the section of this book that deals with deception and compliance tactics, you will notice that many techniques are identified that are also part of normal human interaction. If they are applying these to you systematically, you might get concerned. On the other hand, in Britain there was a recent television show where a wife applied dog training techniques to her husband and her husband was far happier and well behaved in only a few weeks.

6.7.5.3 Do you have other friends you can confide in?

If nothing else it will provide good gossip for them if you discuss any concerns you have in your relationship with friends that were there before you got to know your newest significant other. Talk to your friends if you have any hesitation, or just for the fun of it.

6.7.5.4 Do a background check

This one is pretty radical. Some parents are now doing background checks on the potential spouses their children bring home. Of course wealthy people tend to marry other aristocrats and you can tell them by the homes they own and the boats they have. But the rest of us have to go with criminal records checks and private detectives that follow the potential son-in-law or daughter-in-law. My kids are sure going to hate me when they find out. If they ever actually read my book... There is hope!

6.7.5.5 It's better to have loved and lost

There is an old saying: "It's better to have loved and lost than never to have loved at all." The key is to make sure you don't lose too much. Prenuptial agreements, trust funds for the kids, etc. all help.

6.7.6 Injury frauds

If you don't know that I like to make a little joke now and then, you must have skipped the rest of the book. I'll start out with the best ideas I have but I advise you not to apply them.

6.7.6.1 Why did they pick you?

Most apparent injury fraudsters pick on targets they are likely to be able to win against. Folks with more to lose are more likely to have insurance, so if you drive a new expensive car you are more likely to be targeted. Drive a clunker like I do and nobody will bother you.

6.7.6.2 Make sure your driving is unpredictable

This is my best defense. Drive like a madman and anyone will think twice before risking their life trying to get sideswiped by you. It won't work of course, and nobody really wants to commit vehicular homicide, but it's a thought.

6.7.6.3 Put the really heavy things up top

Here's my last really silly one. In the yank down fraud when you put really heavy things like lead bricks up high, they will get seriously injured, and while you will still have to pay for their care, they will also pay the price for their frauds.

6.7.6.4 Surveillance

Probably the most effective technique available today for countering most injury frauds is a good set of surveillance cameras. These make recordings of the detailed actions and are useful in court. You need to plan on going to court if these sorts of frauds are taken up against you. And you should make sure you get pictures and details and proper medical care for the injured.

6.7.6.5 Histories help

Most injury frauds involve repeat offenders. It's worth checking the history of these fraudsters to see if they have done this before. Local police can help a lot.

6.7.6.6 Private investigators

Reputable private investigation services often catch injury frauds, especially when they go swimming with their supposedly sprained neck or when they go fishing with their lame shoulder.

6.7.7 Help me!

When legitimate people need help you should rush to their aid. But when someone cries for help outside your door, you probably don't want to leave the door opened as you rush out to help them. It's hard to turn down people who need your help. And you should not.

6.7.7.1 The best way to help is with your time

I have always believed that the best way to truly help others is by applying my time to their problem. It turns out that very few frauds are interested in anything but your money, unless you are a good reference for them to get to someone else.

6.7.7.2 Get personally involved

Help frauds involving people you know are best handled by getting personally in touch with the person you are trying to help rather than letting a surrogate do the helping for you. Among other things, it will improve your friendship dramatically if it is a real call for help.

6.7.7.3 How to help at a distance

Do all of us a favor and call the American Red Cross, another charity that you know and trust, your local religious community leaders, or your local government. Find out from them the best way to help others in need. It is sad that this is the way it is, but the fraudsters are out there and hunting for your good deeds.

6.7.8 Help you!

I, for one, need help. My marketing has never been as good as my products and services. But the big difference in getting help is whether you ask for it.

6.7.8.1 Only accept help where you need it

The first rule of getting help is that you should have known you needed it before they asked if they could help you. If you are trying to lose weight, you will find plenty of frauds without them coming to you. But most of us are looking for help in specific ways that the fraudsters may not know about. They try for the least common denominator, so you should only accept help in niches where you need help and it's not worth trying to defraud people.

6.7.8.2 Unless you were already looking

If you are looking for marketing help, you can find a lot of potential helpers without them seeking you out. My point is that getting help should be initiated by you and not by them. If they initiate, you should find out where they got your name. If they are legitimate they will likely be willing to tell you and engage you in a conversation.

6.7.8.3 Interact with people

Which brings me to the human element. I prefer to deal with real people who will take the time to interact with me. For most frauds of this sort the fraudsters don't want to deal with you for very long because they are not looking for a long-term relationship, just a quick hit and run.

6.7.8.4 Take a step at a time

Before you rush headlong into getting help, try going a step at a time. Find out who they are, how they found out about you, their name and address, how to get in touch with them, and so forth.

6.7.8.5 Get and check references

They will all have references, but you can do better. Try getting their address and looking them up. Find out if they are listed in the phone book and where. Do a search to find if there are complaints about them. Call their local better business bureau and chamber of commerce and find out about them. These are all sources that will be happy to help you find out about legitimate businesses and will let you know if there is something suspicious.

6.7.8.6 Go slow and check results

I like to do business with people I know. So I go slow. I start with a small thing here or there and work my way up to larger and larger deals based on the history I have accumulated with them. It takes years to gain reasonable levels of trust adequate to put substantial risks in someone else, but of course what is substantial has a lot to do with how much money you can afford to lose.

6.7.8.7 Watch for compliance tactics

Look out for the tactics of compliance and the patterns I identified earlier. If they are in a rush, take your time. If they become threatening when you try to back off, walk away. If they won't answer the same questions about themselves that they ask about you, walk away.

6.7.9 Other frauds

Most other frauds have common elements with the ones I have already discussed defenses for.

6.7.9.1 Deny it

Chain letters should not be read in the first place and you should ignore anyone who tries to tell you what they said. If someone claims to have known what was in it, identify that it must have been a different chain letter, that was not what yours said. If they claim to have sent it to you, tell them it must have gotten picked up by the postal inspectors because you never got it.

6.7.9.2 Report yourself

The best response to any sort of blackmail attempt is to report it yourself and identify that someone is trying to blackmail you. If it is a legal matter, go to the police or your lawyer. Don't have one? Call the American Bar Association. If it is a business matter go to your management. Getting fired is far better than being blackmailed.

6.7.9.3 Gaming frauds

Stay away from street games of all sorts. Go to a casino if you want to be ripped off systematically and slowly with a chance of walking out a winner and fine food and entertainment along the way.

6.7.9.4 Walk away from the big con

Opportunity will knock again and legitimately. Something for nothing never works and much for little fails most of the time. Recognize the pattern of the big con and don't stay long enough to get caught up in their net.

6.7.10 Call the police

My last and most important piece of advice for the victim of fraud is to call the police. I know it may be embarrassing to report that you got scammed, especially after you have read my book, but suck it up and make the call. You will be helping many others as well as yourself and the rest of society.

I won't lie and tell you that you are likely to get your money back. You probably won't, although it does happen from time to time. But what you will do is help to get the fraudster caught and taken out of your neighborhood, possibly even to jail. And you will be helping the rest of us not get defrauded in the future. And of course, tell everyone else you know to read this book so they will know what to do and the fraudsters will leave your area and end up in jail and eventually give it up. Right...

6.8 Conclusions

This is where I wrap it all up. So I'll keep it simple. Frauds, spies, and lies all use the techniques of deception to take advantage of others. The best defense is to know the enemy and prepare for them.

In the graduate course I teach on deception, perception management, etc. and how to counter them, I face some serious opposition in the University community because, in order to teach about how to defeat them, I have to teach about them. The question that comes up is whether I do more harm than good by teaching people about frauds in order to defeat them and how far I should go in this educational process. Should I have students actually perpetrate frauds to show them how they work? I think this is a bad idea. Should I have them participate in red team exercises in order to understand just how well the techniques work and have them help advise on how to counter them? I think this is a good idea, but lots of folks don't agree.

So I hope I have answered the questions and met the requirements for making this book more of a benefit to those trying to counter frauds than an aid to those trying to perpetrating them. I do know this. People who commit frauds have no problems coming up with and executing their ideas, but the people they defraud seem to have lots of problems being victimized. I hope that this at least starts to level the playing field. Even though it will likely get every fraudster in the world to add me to their list of targets.

Whether it is a politician telling you how they will benefit you, a fraudster telling you how they can make you rich, or a spy telling you that you are the greatest expert they have every seen, by now you know what they do, how they do it, why it works, and what you can do about it.

Good luck.

Detailed Table of Contents