Chapter 1

Kevin's Story

by Kevin Mitnick

I was reluctant to write this section because I was sure it would sound self-serving. Well, okay, it is self-serving. But I've been contacted by literally hundreds of people who want to know "who is Kevin Mitnick."

For those who don't give a damn, please turn to Chapter 2. For everybody else, here, for what it's worth, is the story.

Kevin Speaks

Some hackers destroy people's files or entire bard drives; they're called crackers or vandals. Some novice hackers don't bother learning the technology, but simply download hacker tools to break into computer systems; they are called script kiddies. More experienced hackers with programming skills develop hacker programs and post them to the Web and to bulletin board systems.

And then there are individuals who have no interest in the technology, but use the computer merely as a tool to aid them in stealing money, goods, or services. Despite the media-created myth of Kevin Mitnick, I'm not a malicious hacker. What I did wasn't even against the law when I began, but became a crime after new legislation was passed. I continued anyway, and was caught. My treatment by the federal government was based not on the crimes, but on making an example of me.

I did not deserve to be treated like a terrorist or violent criminal: Having my residence searched with a blank search warrant; being thrown into solitary for months; denied the fundamental Constitutional rights guaranteed to anyone accused of a crime; being denied not only bail but a bail hearing; and being forced to spend years fighting to obtain the government's evidence so my court appointed attorney could prepare my defense.

What about my right to a speedy trial? For years I was given a choice every six months: sign a paper waiving your Constitutional right to a speedy trial or go to trial with an attorney who is unprepared; I chose to sign.

But I'm getting ahead of my story.

Starting Out

My path was probably set early in life. I was a happy-go-lucky kid, but bored. After my father split when I was three, my mother worked as a waitress to support us. To see me

then an only child being raised by a mother who put in long, harried days on a sometimes erratic schedule would have been to see a youngster on his own almost all his waking hours. I was my own babysitter.

Growing up in a San Fernando Valley community gave me the whole of Los Angeles to explore, and by the age of twelve I had discovered a way to travel free throughout the whole greater L.A. area. I realized one day while riding the bus that the security of the bus transfer I had purchased relied on the unusual pattern of the paper-punch that the drivers used to mark day, time and route on the transfer slips. A friendly driver, answering my carefully planted question, told me where to buy that special type of punch.

The transfers are meant to let you change buses and continue a journey to your destination, but I worked out how to use them to travel anywhere I wanted to go for free. Obtaining blank transfers was a walk in the park: the trash bins at the bus terminals were always filled with only-partly-used books of transfers that the drivers tossed away at the end of their shifts. With a pad of blanks and the punch, I could mark my own transfers and travel anywhere that L.A. buses went. Before long, I had all but memorized the bus schedules of the entire system. This was an early example of my surprising memory for certain types of information; still, today I can remember phone numbers, passwords and other items as far back as my childhood.

Another personal interest that surfaced at an early age was my fascination with performing magic. Once I learned how a new trick worked, I would practice, practice, and practice until I mastered it. To an extent, it was through magic that I discovered the enjoyment in fooling people.

From Phone Phreak, to Hacker

My first encounter with what I would eventually learn to call social engineering came about during my high school years, when I met another student who was caught up in a hobby called phone phreaking. Phone phreaking is a type of hacking that allows you to explore the telephone network by exploiting the phone systems and phone company employees. He showed me neat tricks he could do with a telephone, like obtaining any information the phone company had on any customer, and using a secret test number to make long distances calls for free (actually free only to us – I found out much later that it wasn't a secret test number at all: the calls were in fact being billed to some poor company's MCI account).

That was my introduction to social engineering-my kindergarten, so to speak. He and another phone phreaker I met shortly thereafter let me listen in as they each made pretext calls to the phone company. I heard the things they said that made them sound believable, I learned about different phone company offices, lingo and procedures. But that "training"

didn't last long; it didn't have to. Soon I was doing it all on my own, learning as I went, doing it even better than those first teachers.

The course my life would follow for the next fifteen years had been set.

One of my all-time favorite pranks was gaining unauthorized access to the telephone switch and changing the class of service of a fellow phone phreak. When he'd attempt to make a call from home, he'd get a message telling him to deposit a dime, because the telephone company switch received input that indicated he was calling from a pay phone. I became absorbed in everything about telephones-not only the electronics, switches, and computers; but also the corporate organization, the procedures, and the terminology. After a while, I probably knew more about the phone system than any single employee. And, I had developed my social engineering skills to the point that, at seventeen years old, I was able to talk most Telco employees into almost anything, whether I was speaking with them in person or by telephone.

My hacking career started when I was in high school. Back then we used the term hacker to mean a person who spent a great deal of time tinkering with hardware and software, either to develop more efficient programs or to bypass unnecessary steps and get the job done more quickly. The term has now become a pejorative, carrying the meaning of "malicious criminal." In these pages I use the term the way I have always used it - in its earlier, more benign sense.

In late 1979, a group of fellow hacker types who worked for the Los Angeles Unified School
District dared me to try hacking into The Ark, the computer system at Digital Equipment Corporation used for developing their RSTS/E operating system software. I wanted to be accepted by the guys in this hacker group so I could pick their brains to learn more about operating systems.

These new "friends" had managed to get their hands on the dial-up number to the DEC computer system. But they knew the dial-up number wouldn't do me any good: Without an account name and password, I'd never be able to get in.

They were about to find out that when you underestimate others, it can come back to bite you in the butt. It turned out that, for me, even at that young age, hacking into the DEC system was a pushover. Claiming to be Anton Chernoff, one of the project's lead developers, I placed a simple phone call to the system manager. I claimed I couldn't log into one of "my" accounts, and was convincing enough to talk the guy into giving me accessing and allowing me to select a password of my choice.

As an extra level of protection, whenever anyone dialed into the development system, the user also had to provide a dial-up password. The system administrator told me the password. It was "buffoon," which I guess described what he must have felt like later on, when he found out what had happened.

In less than five minutes, I had gained access to Digital's RSTE/E development system. And I wasn't logged on as just as an ordinary user, but as someone with all the privileges of a system developer.

At first my new, so-called friends refused to believe I had gained access to The Ark. One of them dialed up the system and shoved the keyboard in front of me with a challenging look on his face. His mouth dropped open as I matter-of-factly logged into a privileged account. I found out later that they went off to another location and, the same day, started downloading source-code components of the DEC operating system.

And then it was my turn to be floored. After they had downloaded all the software they wanted, they called the corporate security department at DEC and told them someone had hacked into the company's corporate network. And they gave my name. My so-called friends first used my access to copy highly sensitive source code, and then turned me in. There was a lesson here, but not one I managed to learn easily. Through the years to come, I would repeatedly get into trouble because I trusted people who I thought were my friends.

After high school I studied computers at the Computer Learning Center in Los Angeles. Within a few months, the school's computer manager realized I had found a vulnerability in the operating system and gained full administrative privileges on their IBM minicomputer. The best computer experts on their teaching staff couldn't figure out how I had done this. In what may have been one of the earliest examples of "hire the hacker," I was given an offer I couldn't refuse: Do an honors project to enhance the school's computer security, or face suspension for hacking the system. Of course I chose to do the honors project, and ended up graduating Cum Laude with Honors.

Becoming a Social Engineer

Some people get out of bed each morning dreading their daily work routine at the proverbial salt mines. I've been lucky enough to enjoy my work. In particular you can't imagine the challenge, reward, and pleasure I had in the time I spent as a private investigator. I was honing my talents in the performance art called social engineering - getting people to do things they wouldn't ordinarily do for a stranger - and being paid for it.

For me it wasn't difficult becoming proficient in social engineering. My father's side of the family had been in the sales field for generations, so the art of influence and persuasion

might have been an inherited trait. When you combine an inclination for deceiving people with the talents of influence and persuasion you arrive at the profile of a social engineer. You might say there are two specialties within the job classification of con artist. Somebody who swindles and cheats people out of their money belongs to one sub-specialty, the grifter. Somebody who uses deception, influence, and persuasion against businesses, usually targeting their information, belongs to the other sub-specialty, the social engineer.

From the time of my bus transfer trick, when I was too young to know there was anything wrong with what I was doing, I had begun to recognize a talent for finding out the secrets I wasn't supposed to have. I built on that talent by using deception, knowing the lingo, and developing a well-honed skill of manipulation.

One way I used to work on developing the skills in my craft (if I may call it a craft) was to pick out some piece of information I didn't really care about and see if I could talk somebody on the other end of the phone into providing it, just to improve my talents. In the same way I used to practice my magic tricks, I practiced pretexting. Through these rehearsals, I soon found I could acquire virtually any information I targeted.

In Congressional testimony before Senators Lieberman and Thompson years later, I told them, "I have gained unauthorized access to computer systems at some of the largest corporations on the planet, and have successfully penetrated some of the most resilient computer systems ever developed. I have used both technical and non-technical means to obtain the source code to various operating systems and telecommunications devices to study their vulnerabilities and their inner workings." All of this was really to satisfy my own curiosity, see what I could do, and find out secret information about operating systems, cell phones, and anything else that stirred my curiosity.

The train of events that would change my life started when I became the subject of a July 4th, 1994 front-page, above-the-fold story in the New York Times. Overnight, that one story turned my image from a little known nuisance of a hacker into Public Enemy Number One of cyberspace.

John Markoff, the Media's Grifter

"Combining technical wizardry with the ages-old guile of a grifter, Kevin Mitnick is a computer programmer run amok." (The New York Times, 7/4/94.)

Combining the ages-old desire to attain undeserved fortune with the power to publish false and defamatory stories about his subjects on the front page of the New York Times, John Markoff was truly a technology reporter run amok.

Markoff was to earn himself over $1 million by single-handedly creating what I label "The Myth of Kevin Mitnick." He became very wealthy through the very same technique I used to compromise computer systems and networks around the world: deception. In this case however, the victim of the deception wasn't a single computer user or system administrator, it was every person who trusted the news stories published in the pages of the New York Times.

Cyberspace's Most Wanted

Markoff's Times article was clearly designed to land a contract for a book about my life story. I've never met Markoff, and yet he has literally become a millionaire through his libelous and defamatory "reporting" about me in the Times and in his 1991 book, Cyberpunk.

In his article, he included some dozens of allegations about me that he stated as fact without citing his sources, and that even a minimal process of fact-checking (which I thought all first-rate newspapers required their reporters to do) would have revealed as being untrue or unproven.

In that single false and defamatory article, Markoff labeled me as "cyberspace's most wanted," and as "one of the nation's most wanted computer criminals," without justification, reason, or supporting evidence, using no more discretion than a writer for a supermarket tabloid.

In his slanderous article, Markoff falsely claimed that I had wiretapped the FBI (I hadn't); that I had broken into the computers at NORAD (which aren't even connected to any network on the outside); and that I was a computer "vandal," despite the fact that I had never intentionally damaged any computer I ever accessed. These, among other outrageous allegations, were completely false and designed to create a sense of fear about my capabilities.

In yet another breach of journalistic ethics, Markoff failed to disclose in that article and in all of his subsequent articles - a preexisting relationship with me, a personal animosity based on my having refused to participate in the book Cyberpunk In addition, I had cost him a bundle of potential revenue by refusing to renew an option for a movie based on the book.

Markoff's article was also clearly designed to taunt America's law enforcement agencies. "...(L)aw enforcement," Markoff wrote, "cannot seem to catch up with him...." The article was deliberately framed to cast me as cyberspace's Public Enemy Number One in order to influence the Department of Justice to elevate the priority of my case.

A few months later, Markoff and his cohort Tsutomu Shimomura would both participate as defacto government agents in my arrest, in violation of both federal law and journalistic ethics. Both would be nearby when three blank warrants were used in an illegal search of my residence, and be present at my arrest. And, during their investigation of my activities, the two would also violate federal law by intercepting a personal telephone call of mine. While making me out to be a villain, Markoff, in a subsequent article, set up Shimomura as the number one hero of cyberspace. Again he was violating journalistic ethics by not disclosing a preexisting relationship: this hero in fact had been a personal friend of Markoff's for years.

First Contact

My first encounter with Markoff had come in the late eighties when he and his wife Katie Hafner contacted me while they were in the process of writing Cyberpunk, which was to be the story of three hackers: a German kid known as Pengo, Robert Morris, and myself. What would my compensation be for participating? Nothing. I couldn't see the point of giving them my story if they would profit from it and I wouldn't, so I refused to help.

Markoff gave me an ultimatum: either interview with us or anything we hear from any source will be accepted as the truth. He was clearly frustrated and annoyed that I would not cooperate, and was letting me know he had the means to make me regret it. I chose to stand my ground and would not cooperate despite his pressure tactics.

When published, the book portrayed me as "The Darkside Hacker." I concluded that the authors had intentionally included unsupported, false statements in order to get back at me for not cooperating with them. By making my character appear more sinister and casting me in a false light, they probably increased the sales of the book.

A movie producer phoned with great news: Hollywood was interested in making a movie about the Darkside Hacker depicted in Cyberpunk. I pointed out that the story was full of inaccuracies and untruths about me, but he was still very excited about the project. I accepted $5,000 for atwo-year option, against an additional $45,000 if they were able to get a production deal and move forward.

When the option expired, the production company asked for a six month extension. By this time I was gainfully employed, and so had little motivation for seeing a movie produced that showed me in such an unfavorable and false light. I refused to go along with the extension. That killed the movie deal for everyone, including Markoff, who had probably expected to make a great deal of money from the project. Here was one more reason for John Markoff to be vindictive towards me.

Around the time Cyberpunk was published, Markoff had ongoing email correspondence with his friend Shimomura. Both of them were strangely interested in my whereabouts and

what I was doing. Surprisingly, one e-mail message contained intelligence that they had learned I was attending the University of Nevada, Las Vegas, and had use of the student computer lab. Could it be that Markoff and Shimomura were interested in doing another book about me? Otherwise, why would they care what I was up to?

Markoff in Pursuit

Take a step back to late 1992. I was nearing the end of my supervised release for compromising Digital Equipment Corporation's corporate network. Meanwhile I became aware that the government was trying to put together another case against me, this one for conducting counterintelligence to find out why wiretaps had been placed on the phone lines of a Los Angeles P.II firm.

In my digging, I confirmed my suspicion: the Pacific Bell security people were indeed investigating the firm. So was a computer crime deputy from the Los Angeles County Sheriff's Department. (That deputy turns out to be, coincidentally, the twin brother of my co-author on this book. Small world.)

About this time, the Feds set up a criminal informant and sent him out to entrap me. They knew I always tried to keep tabs on any agency investigating me. So they had this informant befriend me and tip me off that I was being monitored. He also shared with me the details of a computer system used at Pacific Bell that would let me do counter-surveillance of their monitoring. When I discovered his plot, I quickly turned the tables on him and exposed him for credit card fraud he was conducting while working for the government in an informant capacity. I'm sure the Feds appreciated that!

My life changed on Independence Day, 1994 when my pager woke me early in the morning. The caller said I should immediately pick up a copy of the New York Times. I couldn't believe it when I saw that Markoff had not only written an article about me, but the Times had placed it on the front page. The first thought that came to mind was for my personal safety-now the government would be substantially increasing their efforts to find me. I was relieved that in an effort to demonize me, the Times had used a very unbecoming picture. I wasn't fearful of being recognized, they had chosen a picture so out of date that it didn't look anything like me!

As I began to read the article, I realized that Markoff was setting himself up to write the Kevin Mitnick book, just as he had always wanted. I simply could not believe the New York Times would risk printing the egregiously false statements that he had written about me. I felt helpless. Even if I had been in a position to respond, I certainly would not have an audience equal to the New York Times to rebut Markoff's outrageous lies.

While I can agree I had been a pain in the ass, I had never destroyed information, nor used or disclosed to others any information I had obtained. Actual losses by companies from my

hacking activities amounted to the cost of phone calls I had made at phone company expense, the money spent by companies to plug the security vulnerabilities that my attacks had revealed, and in a few instances possibly causing companies to reinstall their operating systems and applications for fear I might have modified software in a way that would allow me future access. Those companies would have remained vulnerable to far worse damage if my activities hadn't made them aware of the weak links in their security chain.

Though I had caused some losses, my actions and intent were not malicious ... and then John Markoff changed the world's perception of the danger I represented. The power of one unethical reporter from such an influential newspaper to write a false and defamatory story about anyone should haunt each and every one of us. The next target might be you.

The Ordeal

After my arrest I was transported to the County Jail in Smithfield, North Carolina, where the U.S. Marshals Service ordered jailers to place me into `the hole' - solitary confinement. Within a week, federal prosecutors and my attorney reached an agreement that I couldn't refuse. I could be moved out of solitary on the condition that I waived my fundamental rights and agreed to: a) no bail hearing; b) no preliminary hearing; and, c) no phone calls, except to my attorney and two family members. Sign, and I could get out of solitary. I signed.

The federal prosecutors in the case played every dirty trick in the book up until I was released nearly five years later. I was repeatedly forced to waive my rights in order to be treated like any other accused. But this was the Kevin Mitnick case: There were no rules. No requirement to respect the Constitutional rights of the accused. My case was not about justice, but about the government's determination to win at all costs. The prosecutors had made vastly overblown claims to the court about the damage I had caused and the threat I represented, and the media had gone to town quoting the sensationalist statements; now it was too late for the prosecutors to back down. The government could not afford to lose the Mitnick case. The world was watching.

I believe that the courts bought into the fear generated by media coverage, since many of the more ethical journalists had picked up the "facts" from the esteemed New York Times and repeated them.

The media-generated myth apparently even scared law enforcement officials. A confidential document obtained by my attorney showed that the U.S. Marshals Service had issued a warning to all law enforcement agents never to reveal any personal information to me; otherwise, they might find their lives electronically destroyed.

Our Constitution requires that the accused be presumed innocent before trial, thus granting all citizens the right to a bail hearing, where the accused has the opportunity to be represented by counsel, present evidence, and cross-examine witnesses. Unbelievably, the government had been able to circumvent these protections based on the false hysteria generated by irresponsible reporters like John Markoff. Without precedent, I was held as a pre-trial detainee-a person in custody pending trial or sentencing-for over four and a half years. The judge's refusal to grant me a bail hearing was litigated all the way to the U.S. Supreme Court. In the end, my defense team advised me that I had set another precedent: I was the only federal detainee in U.S. history denied a bail hearing. This meant the government never had to meet the burden of proving that there were no conditions of release that would reasonably assure my appearance in court.

At least in this case, federal prosecutors did not dare to allege that I could start a nuclear war by whistling into a payphone, as other federal prosecutors had done in an earlier case. The most serious charges against me were that I had copied proprietary source code for various cellular phone handsets and popular operating systems.

Yet the prosecutors alleged publicly and to the court that I had caused collective losses exceeding $300 million to several companies. The details of the loss amounts are still under seal with the court, supposedly to protect the companies involved; my defense team, though, believes the prosecution's request to seal the information was initiated to cover up their gross malfeasance in my case. It's also worth noting that none of the victims in my case had reported any losses to the Securities and Exchange Commission as required by law. Either several multinational companies violated Federal law-in the process deceiving the SEC, stockholders, and analysts - or the losses attributable to my hacking were, in fact, too trivial to be reported.

In his book he Fugitive Game, Jonathan Li wan reports that within a week of the New York Times front-page story, Markoff's agent had "brokered a package deal" with the publisher Walt Disney Hyperion for a book about the campaign to track me down. The advance was to be an estimated $750,000. According to Littman, there was to be a Hollywood movie, as well, with Miramax handing over $200,000 for the option and "a total $650,000 to be paid upon commencement of filming." A confidential source has recently informed me that Markoff's deal was in fact much more than Littman had originally thought.

So John Markoff got a million dollars, more or less, and I got five years.

What Others Say

One book that examines the legal aspects of my case was written by a man who had himself been a prosecutor in the Los Angeles District Attorney's office, a colleague of the attorneys who prosecuted me. In his book Spectacular Computer Crimes, Buck Bloombecker wrote, "It grieves me to have to write about my former colleagues in less than

flattering terms.... I'm haunted by Assistant United States Attorney James Asperger's admission that much of the argument used to keep Mitnick behind bars was based on rumors which didn't pan out."

He goes on to say, "It was bad enough that the charges prosecutors made in court were spread to millions of readers by newspapers around the country. But it is much worse that these untrue allegations were a large part of the basis for keeping Mitnick behind bars without the possibility of posting bail?" He continues at some length, writing about the ethical standards that prosecutors should live by, and then writes, "Mitnick's case suggests that the false allegations used to keep him in custody also prejudiced the court's consideration of a fair sentence."

In his 1999 Forbes article, Adam L. Penenberg eloquently described my situation this way: "Mitnick's crimes were curiously innocuous. He broke into corporate computers, but no evidence indicates that he destroyed data. Or sold anything he copied. Yes, he pilfered software but in doing so left it behind." The article said that my crime was "To thumb his nose at the costly computer security systems employed by large corporations." And in the book The Fugitive Game, author Jonathan Littman noted, "Greed the government could understand. But a hacker who wielded power for its own sake ... was something they couldn't grasp."

Elsewhere in the same book, Littman wrote: U.S. Attorney James Sanders admitted to Judge Pfaelzer that Mitnick's damage to DEC was not the $4 million that had made the headlines but $160,000. Even that amount was not damage done by Mitnick, but the rough cost of tracing the security weakness that his incursions had brought to DEC's attention. The government acknowledged it had no evidence of the wild claims that had helped hold Mitnick without bail and in solitary confinement. No proof Mitnick had ever compromised the security of the NSA. No proof that Mitnick had ever issued a false press release for Security Pacific Bank. No proof that Mitnick ever changed the TRW credit report of a judge.

But the judge, perhaps influenced by the terrifying media coverage, rejected the plea bargain and sentenced Mitnick to a longer term then even the government wanted. Throughout the years spent as a hacker hobbyist, I've gained unwanted notoriety, been written up in numerous news reports and magazine articles, and had four books written about me. Markoff and Shimomura's libelous book was made into a feature film called Takedown. When the script found its way onto the Internet, many of my supporters picketed Miramax Films to call public attention to the inaccurate and false characterization of me. Without the help of many kind and generous people, the motion picture would surely have falsely portrayed me as the Hannibal Lector of cyberspace. Pressured by my supporters, the production company agreed to settle the case on confidential terms to avoid me filing a libel action against them.

Final Thoughts

Despite John Markoff's outrageous and libelous descriptions of me, my crimes were simple crimes of computer trespass and making free telephone calls. I've acknowledged since my arrest that the actions I took were illegal, and that I committed invasions of privacy. But to suggest, without justification, reason, or proof, as did the Markoff articles, that I had deprived others of their money or property by computer or wire fraud, is simply untrue, and unsupported by the evidence.

My misdeeds were motivated by curiosity: I wanted to know as much as I could about how phone networks worked, and the ins and outs of computer security. I went from being a kid who loved to perform magic tricks to becoming the world's most notorious hacker, feared by corporations and the government. As I reflect back on my life for the last thirty years, I admit I made some extremely poor decisions, driven by my curiosity, the desire to learn about technology, and a good intellectual challenge.

I'm a changed person now. I'm turning my talents and the extensive knowledge I've gathered about information security and social engineering tactics to helping government, businesses and individuals prevent, detect, and respond to information security threats. This book is one more way that I can use my experience to help others avoid the efforts of the malicious information thieves of the world. I think you will find the stories enjoyable, eye opening and educational.

– *Kevin Mitnick*