**Kevin Mitnick Case: 1999**

[Great American Trials](http://www.encyclopedia.com/Great%2BAmerican%2BTrials/publications.aspx?pageNumber=1) | 2002 | Smith, Tom | 700+ words | COPYRIGHT 2002 Thomson Learning. (Hide copyright information)[Copyright](http://www.encyclopedia.com/doc/1G2-3498200381.html)

**Kevin Mitnick Case: 1999**

**Defendant:** Kevin D. Mitnick
**Crimes Charged:** Wire fraud (14 counts), possession of unauthorized access devices (8 counts), interception of wire or electronic communications, unauthorized access to a federal computer, and causing damage to a computer
**Chief Defense Lawyers:** Donald Randolph and Gregory Vincent
**Chief Prosecutors:** Christopher Painter and David Schindler
**Judge:** Marianna Pfaelzer
**Place:** Los Angeles, California
**Date of Sentencing after Plea Agreement:** August 10, 1999
**Plea:** Guilty
**Sentence:** 3 years and 10 months imprisonment, plus 3 years probation with strict limitations on use of computer equipment

**SIGNIFICANCE:** The federal prosecution of computer "hacker" Kevin Mitnick was the first case to focus international attention on computer security issues.

When the FBI arrested him on February 15, 1995, in a Raleigh, North Carolina, apartment, Kevin Mitnick was either a master of victimless computer trespassing or a dangerous vandal whose intrusions into commercial computer sites had cost international companies millions of dollars. The argument over whether Mitnick was a felon or a mere nuisance would outlast his confrontation with the justice system.

Prior to his North Carolina arrest, Mitnick was already well known to the authorities and had previously been prosecuted numerous times for "hacking" or using the Internet to gain unauthorized access to computers. In 1981, as a teenager, he was convicted of burgling computer manuals from Pacific Bell and sentenced to probation. He served six months in jail in 1983 for breaking into computers at the University of Southern California. In 1987 he was arrested for hacking into the computers of a Santa Cruz software publisher and sentenced at that time to three years probation. In 1988, Mitnick was arrested for illegally copying software from Digital Equipment Corporation. During that trial, his defense attorneys argued that his hacking activities were an "addiction" and he was sentenced to a year in jail and six months in a halfway house.

In 1992, authorities planned to arrest Mitnick for hacking into Pacific Bell computers and for violating the terms of his parole by associating with Lewis DePayne, a longtime friend and also a convicted hacker. Alerted to the impending arrest, Mitnick disappeared. His hacking, however, continued. After he attacked the computers of California computer security expert Tsutomu Shimomura, Shimomura assisted the FBI in tracking Mitnick to North Carolina.

By the time Mitnick and DePayne were taken into custody in 1995, the federal government had compiled a substantial indictment against them: 25 counts of computer crimes including possession of unauthorized access devices, computer fraud, causing damage to computers, wire fraud, and interception of wire or electronic communications. The indictment accused the pair of fraudulently obtaining unauthorized access to computers belonging to software and operating systems manufacturers, cellular telephone manufacturers, internet service providers, and educational institutions. They allegedly used the information to steal and copy proprietary computer software from Motorola, Nokia, Fujitsu, Novell, NEC, and Sun Microsystems. Mitnick and DePayne were also charged with fraudulent acquisition and possession of hundreds of confidential computer passwords.

**No Bail, No Computer**

When Mitnick was arraigned in Los Angeles on September 30, 1996, he pleaded not guilty. He was denied bail. Mitnick and his lawyer, Donald Randolph, protested that Mitnick should not be denied bail for what they considered to be a benign violation of the law, but prosecutors continued to convincingly portray him as a "flight" risk. Although Randolph appealed the denial of bail all the way to the U.S. Supreme Court, Mitnick remained in prison for nearly five years.

The two sides also fought over Mitnick's right to use a laptop computer in jail to review the voluminous evidence prosecutors planned to use against him. The government argued that Mitnick's facility with computers made him too dangerous to be trusted with one. After over a year of ruling for the prosecution on the matter, Judge Marianna Pfaelzer eventually allowed Mitnick to use a laptop without a modem to review evidence on unalterable CD-ROM discs. The arguing continued, however, over the government's refusal to allow Mitnick access to encrypted data found in his computers at the time of his arrest.

As procedural disputes continued for years, public support for Mitnick among the hacker community grew, highlighting the division of opinion over the exact nature of his offenses. Mitnick's supporters accused the government of persecuting him for what they viewed as a victimless crime. They correctly pointed out that, unlike some hackers, Mitnick had merely copied the information he had accessed and had never used his intrusions into computer systems for financial profit. The companies whose systems he had entered, the government, and his detractors in the computer world, however, accused Mitnick of costing his victims millions of dollars in repairs by breaching their security systems. Supporters cynically responded that Mitnick had done the companies a favor by forcing them to fix the security flaws. Mitnick's defense attorneys accused the government of inflating alleged damage estimates to strengthen the prosecution's case.

**Hacker Pleads Guilty**

A month before Mitnick's trial was finally scheduled to begin on April 20, 1999, he agreed to plead guilty to 5 of the 25 felony counts against him. While Mitnick awaited sentencing, DePayne also agreed to a plea bargain. On April 26, he pleaded guilty to I count of wire fraud and agreed to cooperate with computer security investigators working on the case. He was sentenced to six months of detention at his home.

Although Mitnick's plea was sure to reduce the prison time he risked serving had he been convicted in a federal trial, he still faced a state charge of illegally accessing California Department of Motor Vehicles computers in 1992 to obtain confidential information. On August 6, however, the Los Angeles district attorney's office reversed their long-standing intention to prosecute and dropped the case, saying that Mitnick had been "mischarged." Mitnick had obtained the information over the telephone by simply misidentifying himself as a welfare fraud inspector. Since he had not used a computer, the case against him was unprosecutable and was dismissed upon the request of the D.A.'s office.

His guilty plea in the federal case was ultimately unaffected by the disposition of the unrelated state charge. On August 10, 1999, Judge Pfaelzer sentenced Mitnick to three years and 10 months in prison, granting him credit for time served, to be followed by three years of probation. Prosecutors wanted Mitnick to pay $1.5 million in damages to the companies in whose computer systems he had created so much havoc. The judge instead ordered Mitnick to pay a "token restitution" of $4,125.

Most significant, the terms of Mitnick's three-year probation prohibited him from having any contact with Internet access, computers, software, or cellular telephones. He was also prohibited from working as a computer consultant. Mitnick and his lawyers protested that this would deny him the ability to earn a living, not only in the field that he knew best, but also in a world where computers were increasingly used everywhere, even in the lowliest retail jobs. The judge was unmoved. Mitnick returned to prison to serve the remainder of his sentence.

After being paroled and released on January 21, 2000, Mitnick continued to insist that his hacking activities stemmed from intellectual curiosity about telephone systems and computer security, rather than any fraudulent intentions. And even on parole, his expertise was sufficient for him to be called upon by the media and even the government for his opinions on crimes by less-benign hackers.

—*Tom* *Smith*