

Who is Kevin Mitnick?

Kevin David Mitnick (born August 6, 1963) is a computer security consultant, author and hacker who was sentenced to 5 years in prison for many computer-related and communications crimes.

Kevin David Mitnick (born August 6, 1963) is a computer security consultant, author and hacker who was sentenced to 5 years in prison for many computer-related and communications crimes.

Mitnick's arrest, trial and sentencing, along with related articles, books and movies, has been controversial.

He currently runs security company Mitnick Security Consulting, LLC. Mitnick is also the director of hacking at security awareness training company KnowBe4, and a member of the advisory board at Zimperium, a company that develops mobile intrusion prevention systems.

Learn about Kevin Mitnick

1. Life and career
 1. Childhood
 2. "Career" computer hack
 3. Arrest, conviction, and imprisonment
 4. The controversy involved
 5. Security consulting career
2. The media
3. Books
 1. Written by Mitnick
 2. Authorized by Mitnick

Life and career

Childhood

Mitnick was born in Van Nuys, California on August 6, 1963. He grew up in Los Angeles and studied at James Monroe High School, California. During that time, Mitnick became the operator of an Amateur radio (also known as Ham radio, using non-commercial radio frequency bands such as entertainment, information exchange, testing, training). , etc .). Later, he enrolled at Pierce College in Los Angeles and USC (University of Southern California). For a while, he worked as a receptionist for Stephen S. Wise Temple.

"Career" computer hack

At the age of 12, Mitnick used social engineering and dumpster diving (looking for information written on paper or computer print or in the trash) to defeat the punch card system, used in the bus system. in Los Angeles.

After persuading a bus driver to tell him where to buy a ticket puncher (with the reason that it was for "a school project"), Mitnick could take the bus in the area. LA area, using unused tickets he found in a landfill next to the bus company garage. This social engineering technique then became the main method for obtaining information, including username, password and modem phone number.

The first time Mitnick succeeded in gaining unauthorized access to a computer network was in 1979, when he was just 16 years old, when a friend gave him the phone number of Ark, the Digital Corporation Corporation (DEC) computer system. used to develop RSTS / E operating system software. Mitnick broke into DEC's computer network and then copied their software.

Mitnick was charged and sentenced in 1988. The final sentence was 12 months in prison and 3 years under house arrest after being released. Near the end of his probation, Mitnick broke into Pacific Bell's voicemail computer. After the arrest warrant, Mitnick fled, becoming a wanted criminal for two and a half years.

According to the US Department of Justice, Mitnick gained unauthorized access to dozens of computer networks while fleeing. He used a clone phone to conceal his location and copied valuable proprietary software from some of the country's largest phone companies, as well as computers. Mitnick also steals computer passwords, changes the computer network and reads private emails.

Arrest, conviction, and imprisonment



Supporters from the 2600 magazine sparked the "Free Kevin" movement (roughly translated as 'Please release Kevin').

Following the cult pursuit, the FBI arrested Mitnick on February 15, 1995, in an apartment in Raleigh, North Carolina, for federal violations related to computer hacks over the past two and a half years. . Mitnick was found with the phone, along with more than 100 clone phone codes and many fake documents.

In December 1997, Yahoo! The website is believed to have been hacked, displaying a notice calling for the release of Mitnick, otherwise an Internet "disaster" will occur on Christmas. Yahoo! Answer that the worm does not exist and there are claims that it is just a hoax to scare people.

Mitnick was charged with wire fraud (deceiving others by using television, radio, and Internet links between different locations) (14 counts), possession of retrieval devices. unauthorized access (8 counts), wire or electronic communications, unauthorized access to a federal computer and damage to the computer.

In 1999, Mitnick pleaded guilty to four wire fraud cases, two counts of computer fraud and one charge of blocking illegal communications. Mitnick was sentenced to 46 months in prison, plus 22 months for violating the terms of enforcing probation after his release in 1989, for computer fraud. calculated to retrieve, change electronic data or illegally use computers, systems). He acknowledged violating the terms of the post-release probation, by hacking into Pacific Bell voicemail and other systems, as well as linking with some hackers, in this case co-financing. Pham, defendant Lewis De Payne.

Mitnick was sentenced to 5 years in prison - 4 and a half years before trial and 8 months in solitary confinement - because according to Mitnick, law enforcement officials convinced a judge that, Mitnick could somehow interfere with the NORAD modem via phone from the prison, and communicate with the modem by whistling to launch a nuclear missile.

Mitnick was released on January 21, 2000. During his post-release detention period, which ended on January 21, 2003, he was initially banned from using any communication technology other than landline phones. specified. Mitnick fought against this decision in court, eventually winning a favorable judgment, allowing him access to the Internet. Under the agreement, Mitnick was also banned from making films or books based on its criminal activity for 7 years.

In December 2002, an FCC judge ruled that Mitnick had completed the renovation and was eligible to own a federally issued Amateur radio license. Mitnick currently runs Mitnick Security Consulting LLC, a computer security consultancy company and co-owner of KnowBe4, an integrated platform provider for training in security awareness and phishing testing.

The controversy involved

The offenses, arrests and trials of Mitnick, along with related press publications, are controversial. Although Mitnick was convicted of illegally copying software, his supporters said the penalty was too high, plus many accusations against Mitnick were fraudulent. fraud and is not based on actual losses.

In his 2002 book, *The Art of Deception*, Mitnick said that he only used passwords and code obtained by social engineering. He claimed that he did not use software programs or hacking tools to crack passwords, or exploit computer or phone security.

John Markoff and Tsutomu Shimomura wrote the *Takedown* book on Mitnick's arrest. Later, Jonathan Littman wrote *The Fugitive Game* as a response, accusing:

1. The improper conduct of Markoff, who reported the case to the New York Times, was based on rumors and government statements, while never interviewing Mitnick himself.
2. Excessive government prosecution against Mitnick
3. Orthodox media exaggerates the real crime of Mitnick
4. Shimomura's involvement in this incident is unclear or questionable in legality.

Further controversy over the release of *Track Down* (*Takedown* outside the United States), based on the book by John Markoff and Tsutomu Shimomura, arose when Littman assumed parts of the film were taken from the book. without your permission. The lawsuit against Mitnick has tried many new laws, which are enacted to

handle computer crimes and contribute to raising public awareness about security related to networked computers. However, controversy remains, and today, Mitnick's story is often cited as an example of the impact that mainstream newspapers can have on law enforcement officials.

Security consulting career



Since 2000, Mitnick has been a paid security consultant, speaker, and author. He works as a security consultant for Fortune 500 and FBI companies, conducts penetration testing services for the world's largest companies and teaches Social Engineering classes to dozens of companies, as well as government agencies. .

The media



In 2000, Skeet Ulrich and Russell Wong played Kevin Mitnick and Tsutomu Shimomura in the movie Track Down (called Takedown outside of the United States), based on the book Takedown by John Markoff and Tsutomu Shimomura. The DVD was released in September 2004. A documentary called Freedom Downtime

was produced by 2600: The Hacker Quarterly in response to Takedown.

On August 18, 2011, Mitnick appeared on The Colbert Report to talk about his new book, Ghost in the Wires. On August 23, Mitnick was interviewed on Coast to Coast AM in "Hacking & Technology". On August 24, he appeared on the episode Triangulation of TWiT.tv.



On September 12, 2011, Mitnick answered readers' questions on technology news site Slashdot. This is the second time he has been interviewed on Slashdot (the first time was in February 2003).

Mitnick's story is part of the inspiration for Wizzywig, the graphic novel by Ed Piskor about hackers.

Mitnick also appeared in Werner Herzog's documentary Lo and Behold, Reveries of the Connected World (2016).

Books



Written by Mitnick

Mitnick is a co-author, along with William L. Simon and Robert Vamosi, in his three books on computer security and his autobiography:

1. The Art of Deception: Controlling the Human Element of Security (2003)
2. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers (2005)
3. Ghost in the Wires: My Adventures as the World's Most Wanted Hacker (2011)
4. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data (2017)

Authorized by Mitnick

1. The Fugitive Game: Online with Kevin Mitnick (1996).

In this book, author Jonathan Littman presented the story according to Mitnick's own account, because the book "Takedown" by John Markoff (1996) and "Cyberthief and the Samurai" by Jeff Goodell (1996) presented From Shimomura's point of view (because Mitnick couldn't make money legally from his own story then).

You finished reading the article "**Who is Kevin Mitnick?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.