

# 9 most famous hacking incidents in history

PCMag experts evaluated high-tech crimes based on a number of criteria and below are nine of the most famous high-tech crime cases in history.



PCMag experts evaluate high-tech crimes based on a number of criteria: *sophistication* (there has been a similar case happening before or not), *influence* (number of websites, computers, affected agencies, businesses ..), *damage* (total value of cash losses caused by the attack), *historical impact* (the attack has created a new trend in the world technology or not).

Here are nine of the most famous high-tech crime cases in history.

## John Draper

Famous for the name ' *Cap'n Crunch* ', John Draper is one of the first humans in the world to be ' *named a hacker* '. In the 1970s, Draper used a toy whistle included in the box of Cap'n Crunch cereal to 'hack' into the phone line and freely make 'free' calls.

Draper unknowingly realized that the whistle produced a sound with the same frequency as the call signal frequency on the phone line. Thanks to that, he was able to control the ongoing call that the audience still thought the call was over. In 1972, Draper was discovered when the phone company ' *saw an abnormality* ' in his phone bill. Then Draper was sentenced to 2 months in prison.

Draper's attack was born as the term 'Phreaking'. The meaning of this term in our society today is '*attack on telecommunications systems*'.

### **Kevin Mitnick**

When 17-year-old Kevin Mitnick began to be known. But 3 years later (1983), the name Kevin Mitnick became really popular not only in hackers but also in defense of high-tech crime.

That was the year Mitnick successfully broke into the ARPANet network - the predecessor of the Internet today, but at that time it was only applied to large enterprises, universities and US military forces. Since then, Mitnick has access to the Pentagon network and all US Department of Defense files. However, Mitnick does not retrieve any data.

After the attack was discovered by network administrators, Mitnick was arrested and lived in a juvenile education center for a short time. This is the first hacker case in history to be sentenced to jail for illegally breaking into computers. But for Mitnick, this is the second arrest with the same crime. From then on, Mitnick was constantly under FBI supervision but he was still "comfortable" to carry out a series of subsequent attacks. Continued arrest, investigation, and trial.

### **Robert Morris**

In 1988, a 23-year-old Cornell graduate student Robert Morris distributed 99 lines of malicious code known as the infectious Morris Worm and caused a series of PCs in various countries to stop work. The goal of this hacker is to count the number of PCs connected to the Internet and thereby know how big the Internet is.

This action caused Morris to be arrested in 1989 and became the first person to be convicted under the Computer Abuse Act and to use computers for fraudulent purposes passed by the US Congress in 1986. In addition Morris also had to pay a fine of up to \$ 10,000.

### **Kevin Poulsen**

In 1989, Kevin Poulsen was arrested on charges of unauthorized computer and phone server intrusion. However, just before he was brought to trial, Poulsen escaped and carried out an allegedly most famous attack during the "hacker life."

KIIS-FM Los Angeles Radio that year held a contest with the prize of a Porsche sports car worth 944-S2 for the 102th person to call the radio. Poulsen managed to take control of the switchboard line, block all incoming calls and become the winner. In 1991, Poulsen was arrested at a supermarket in Los Angeles.

### **Vladimir Levin**

In 1994, Vladimir Levin for the first time in the world successfully carried out an illegal transfer of a large sum of money out of a reputable bank. Levin has stolen a series of large corporate bank accounts in the United States through analog wire transfer network of Citibank. The hacker has transferred a total of 10.7 million dollars to a variety of accounts in the US, Finland, Netherlands, Israel and Germany.

Levin's three accomplices were arrested when withdrawing money from banks, but Levin alone had to be arrested by law enforcement agencies in 1995 at Stansted Airport (London, England). In 1997, Levin was extradited to the US, sentenced to 3 years in prison and compensated for Citibank a sum of up to 240,015 USD.

About the stolen money, CitiBank can only retrieve about 400,000 USD.

### **David Smith**

In 1999, David Smith spread Melissa worm from a computer in the state of New Jersey (USA) through a stolen AOL email account. The computer worm is able to automatically spread to the first 50 people named in the Outlook address book when it has infected the PC.

Melissa infected and attacked PCs of more than 300 businesses worldwide - including big names like Microsoft, Intel or Lucent Technologies. These businesses were forced to close their email servers (email gateways) due to too many emails being sent. The total damage caused by Melissa is estimated at \$ 80 million.

After being convicted, Smith was sentenced to 20 months in prison and had to work under the supervision of the FBI to help the agency discover new types of malware as well as their author search.

### **Jonathan James**

At the end of June 1999, Jonathan James dazzled by knowing that NASA's source code could be sold for \$ 1.7 million. James - then only 15 years old - successfully broke into NASA computers by stealing a login account password at the Marshall (Alabama, USA) Space Center in hopes of making some money. whether to sell for money.

The consequences of the attack were that in July 1999 NASA was forced to disconnect from the computer network for several weeks. Stolen documents are documents related to environmental control on the space station such as temperature, humidity . At the age of 16, James was sentenced to 6 months in prison and had to accept the time to supervise challenges until when are 18 years old.

### **MafiaBoy**

At the time of the famous attack, Mike Calce was only known by the name of MafiaBoy by Canadian law enforcement agencies that banned the media from revealing his real name. In February 2000, using 75 PCs on 52 different networks, Calce organized a huge Denial-of-Service attack that took down 10 websites of well-known companies. like Amazon, eBay, E \* TRADE, DELL . There are not any official damage figures published. Analysts estimate that losses can reach up to 1.7 billion Canadian dollars (based on the present value of about 1.6 billion USD).

In 2001, Calce was put on trial and sentenced to 8 months in prison, a year of trial, restricted use of the Internet and had to pay a small sum of money.

### **Gary McKinnon**

For two consecutive years 2001 and 2002, the British hacker broke into the computer networks of the US Department of Defense, the Pentagon, NASA, the naval forces and the US air force in search of evidence of UFOs. Officials claimed the losses of these attacks amounted to \$ 700,000.

McKinnon is currently facing extradition to the US for trial. If convicted, this hacker may have to pay a fine of up to 70 years in prison.

You finished reading the article "**9 most famous hacking incidents in history**" 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.

---