Top Ten Most Notorious (Infamous) Hackers of All Time

Hacking costs companies and consumers many millions of dollars each year. According to Venture Beat, the frequency of attacks on American companies has prompted a steep rise in the cost of cyber-insurance. Much of the problem stems from the advent of the internet, so amateur hackers can find all the tools they need online at virtually no cost. But this proliferation of hacking didn't emerge overnight—it took the work of the now-famous hackers to discover critical vulnerabilities and expose key weaknesses, establishing the foundation of a free-for-all Internet. Here's a look at the top ten most notorious hackers.

1. **Kevin Mitnick**

   A seminal figure in American hacking, Kevin Mitnick got his start as a teen. In 1981, he was charged with stealing computer manuals from Pacific Bell. In 1982 he hacked the North American Defense Command (NORAD), which inspired the 1983 film "War Games." In 1989, he hacked Digital Equipment Corporation's (DEC) network and made copies of their software. Because DEC was a leading computer manufacturer at the time, this act put Mitnick on the map. He was later arrested, convicted and sent to prison. During his conditional release, he hacked Pacific Bell's voicemail systems.

   Throughout his hacking career, Mitnick didn't exploit the access and data he'd obtained. While it's widely believed that he once obtained full control of Pacific Bell's

was in hiding for more than two years. When caught, he went to prison for multiple counts of wire fraud and computer fraud. Mitnick ultimately went white hat, but according to Wired, in 2014, he launched "Mitnick's Absolute Zero Day Exploit Exchange," which sells unpatched, critical software exploits to the highest bidder.

2. **Anonymous**

Anonymous got its start in 2003 on 4chan message boards in an unnamed forum. The group exhibits little organization and is loosely focused on the concept of social justice. For example, in 2008 the group took issue with the Church of Scientology and begin disabling their websites, thus negatively impacting theirs search rankings in Google and overwhelming its fax machines with all-black images. In March 2008, a group of "Anons" marched passed Scientology centers around the world wearing the now-famous Guy Fawkes mask. As noted by The New Yorker, while the FBI and other law enforcement agencies have tracked down some of the group's more prolific members, the lack of any real hierarchy makes it almost impossible to eliminate Anonymous as a whole.

3. **Adrian Lamo**

In 2001, 20-year-old Adrian Lamo used an unprotected content management tool at Yahoo to modify a Reuters article and add a fake quote attributed to former Attorney General John Ashcroft. Often, Lamo would hack systems and then notify both the press and his victims — in some cases, he'd help clean up the mess to improve their security. As Wired points out, however, Lamo took things too far in 2002, when he hacked The New York Times' intranet, added himself to the list of expert sources and began conducting research on high-profile public figures. Because he preferred to wander the streets with little more than a backpack and often had no fixed address, Lamo earned the moniker "The Homeless Hacker."

In 2010, 29-year-old Lamo learned he had Asperger's Disorder, a mild form of Autism often called "geek syndrome" because people with Asperger's have trouble with simple social interactions and display odd, highly focused behavior. Many experts believe this explains Lamo's entry into the world of hacking culture — Asperger's Disorder is reportedly prevalent among the hacking community.

4. **Albert Gonzalez**

According to the New York Daily News, Gonzalez, dubbed "soupnazi," got his start as the "troubled pack leader of computer nerds" at his Miami high school. He eventually became active on criminal commerce site Shadowcrew.com and was considered one of its best hackers and moderators. At 22, Gonzalez was arrested in New York for debit card fraud related to stealing data from millions of card accounts. To avoid jail time, he became an informant for the Secret Service, ultimately helping indict dozens of Shadowcrew members.

accounts from companies including OfficeMax, Dave and Buster's and Boston Market. The New York Times Magazine notes that Gonzalez's 2005 attack on US retailer TJX was the first serial data breach of credit information. Using SQL injection, this famous hacker and his team created back doors in several corporate networks and stole an estimated $256 million from TJX alone. During his sentencing in 2015, the federal prosecutor called Gonzalez's human victimization "unparalleled."

5. **Matthew Bevan and Richard Pryce**

Matthew Bevan and Richard Pryce are a team of British hackers who hacked into multiple military networks in 1996, including Griffiss Air Force Base, the Defense Information System Agency and the Korean Atomic Research Institute (KARI). Bevan (Kuji) and Pryce (Datastream Cowboy) have been accused of nearly starting a third world war after they dumped KARI research onto American military systems. Bevan claims he was looking to prove a UFO conspiracy theory, and according to the BBC, his case bears resemblance to that of Gary McKinnon. Malicious intent or not, Bevan and Pryce demonstrated that even military networks are vulnerable.

6. **Jeanson James Ancheta**

Jeanson James Ancheta had no interest in hacking systems for credit card data or crashing networks to deliver social justice. Instead, Ancheta was curious about the use of bots — software-based robots that can infect and ultimately control computer systems. Using a series of large-scale "botnets," he was able to compromise more than 400,000 computers in 2005. According to Ars Technica, he then rented these machines out to advertising companies and was also paid to directly install bots or adware on specific systems. Ancheta was given 57 months in prison, and his sentence marked the first time a hacker was sent to jail for the use of botnet technology.

7. **Michael Calce**

In February 2000, 15-year-old Michael Calce, also known as "Mafiaboy," discovered how to take over networks of university computers and used their combined resources to disrupt the number-one search engine at the time: Yahoo. Within a week, he'd also brought down Dell, eBay, CNN and Amazon using a dedicated denial of service (DDoS) attack that overwhelmed corporate servers and caused websites to crash. Calce's wake-up call was perhaps the most jarring for investors and Internet proponents. If the biggest website in the world — valued at over $1 billion — could be so easily sidelined, was any online data truly safe? It's not an exaggeration to say that the development of cybercrime legislation suddenly became a top government priority thanks to Calce's hack.

8. **Kevin Poulsen**

to prosecute Poulsen, who was a minor at the time and he was let off with a warning.

Poulsen didn't heed this warning and continued hacking. In 1988, Poulsen hacked a federal computer and dug into files pertaining to the deposed president of the Philippines, Ferdinand Marcos. Discovered by authorities, Poulsen went underground. While he was on the run, Poulsen kept busy, hacking government files and revealing secrets. According to his own website, in 1990, he hacked a radio station contest and ensured that he was the 102nd caller, winning a brand new Porsche, a vacation, and $20,000.

Paulsen was soon arrested and barred from using a computer for three years. He has since reinvented himself as a serious journalist, writing about computer security as the senior editor at Wired.

9. Jonathan James

Using the alias cOmrade, Jonathan James hacked into several companies. But according to the New York Times, what really earned him attention was his hack into the computers of the United States Department of Defense. What was all the more startling was that James was only 15 at the time. In an interview with PC Mag, James admitted that he was partly inspired by the book The Cuckoo's Egg, which details the hunt for a computer hacker in the 1980s. His hacking allowed him to access over three thousand messages from government employees, user names, passwords, and other sensitive data.

James was arrested in 2000 and was sentenced to a six months house arrest and banned from recreational computer use. However, a probation violation caused him to serve six months in jail. Jonathan James became the youngest person to be convicted of violating cybercrime laws.

In 2007, TJX, a department store, was hacked and many customer's private information were compromised. Authorities suspected James might be involved despite a lack of evidence. Johnathan James eventually killed himself by gunshot in 2008. According to the Daily Mail, James wrote in his suicide note, "I have no faith in the 'justice' system. Perhaps my actions today, and this letter, will send a stronger message to the public. Either way, I have lost control over this situation, and this is my only way to regain control."

10. ASTRA

This hacker is different from the others on this list in that he has never been publicly identified. However, according to the Register some information has been released about ASTRA, namely that when he was apprehended by authorities in 2008, he was a 58-year old Greek mathematician. Reportedly, he had been hacking into the Dassault Group, for almost half a decade. During that time, he stole cutting edge

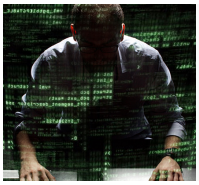
exactly why his true identity has not been revealed but the word Astra is a Sanskrit word for 'weapon'.

11. Some of these top hackers aimed to make the world a better place, others to prove UFO theories. Some wanted money and some hoped for fame, but all played a critical role in the evolution of cybersecurity.

FEATURED ARTICLES


Inoperable Computers and System Networks

Naikon Targeted Attacks


Computer Vandalism


What is a Trojan Virus? - Definition


What to Do if Your Identity is Stolen: A Step-By-Step Guide