Top Ten Hackers

1.Kevin Mitnick

Kevin Mitnick, a prominent individual in the field of American hacking, began his professional journey during his adolescence. In the year 1981, the individual in question faced charges pertaining to the act of unlawfully acquiring computer manuals from Pacific Bell. In the year 1982, the individual successfully gained unauthorized access to the North American Defense Command (NORAD), an accomplishment that served as a source of inspiration for the creation of the film War Games in 1983. In the year 1989, the individual engaged in unauthorized access to the network of Digital Equipment Corporation (DEC) and proceeded to duplicate their software. Due to DEC's prominent position as a computer maker during that period, Mitnick's recognition significantly increased as a result of this move. Subsequently, he was apprehended, found guilty, and subsequently incarcerated. While on conditional release, the individual engaged in unauthorized access to Pacific Bell's voicemail systems.

During the course of his hacking endeavors, Mitnick consistently refrained from utilizing the access and data he acquired for exploitative purposes. There is a prevailing belief that he successfully achieved complete control over Pacific Bell's network with the sole intention of demonstrating its vulnerability to unauthorized access.

2. Anonymous

The origins of Anonymous may be traced back to the year 2003, when it first emerged inside the context of 4chan message boards, specifically within an undisclosed topic. The collective demonstrates a limited
organizational structure and maintains a loosely defined focus on the notion of social justice. In 2008, the aforementioned organization expressed its concerns with the Church of Scientology by engaging in activities such as deactivating its websites. Consequently, this action had adverse effects on the search ranks of the Church in Google, as well as inundating its fax machines with photos consisting solely of black color.

3. Adrian Lamo

Adrian Lamo
In the year 2001, someone
named Adrian Lamo, who was 20 years old at the time, employed an unsecured content management tool on the Yahoo platform to manipulate a Reuters article. This manipulation involved the inclusion of a fabricated quote falsely ascribed to former Attorney General John Ashcroft. Lamo frequently engaged in unauthorized access to computer systems, afterward informing both the media and the affected parties.

In certain instances, he would assist in the remediation of the situation in order to enhance their level of security. According to Wired, Lamo's actions in 2002 went beyond acceptable boundaries. He engaged in unauthorized access to The New York Times intranet, where he proceeded to include himself as an expert source and initiated investigations on prominent public people. Lamo acquired the epithet “The Homeless Hacker” because of his inclination to traverse urban areas with little possessions, typically limited to a bag, and frequently lacking a permanent residential location.

4. Albert Gonzalez

Albert Gonzalez
As reported by the New York Daily News, Gonzalez, who is commonly referred to as "soupnazi," initially gained prominence as the leader of a group of computer enthusiasts with various challenges at his high school in Miami. Subsequently, he became involved in illicit activities on the online platform Shadowcrew.com, where he garnered recognition as one of its most proficient hackers and moderators.

At the age of 22, Gonzalez was apprehended in New York on charges of engaging in debit card fraud, specifically including the illicit acquisition of data from a substantial number of card accounts. In order to evade incarceration, the individual in question assumed the role of an informant for the Secret Service, facilitating the indictment of numerous members associated with the Shadowcrew.

Throughout his tenure as a compensated informant, Gonzalez persisted in engaging in illicit behaviors. Gonzalez, in collaboration with a cohort of associates, illicitly acquired in excess of 180 million payment card accounts from various corporate entities, such as OfficeMax, Dave and Buster's, and Boston Market. During the sentence proceedings in 2015, the federal prosecutor characterized Gonzalez's perpetration of harm against individuals as being of an unprecedented nature.

5. Matthew Bevan and Richard Pryce

In 1996, Matthew Bevan and Richard Pryce, a duo of British hackers, successfully infiltrated several military networks, namely Griffiss Air Force Base, the Defense Information System Agency, and the Korean Atomic Research Institute (KARI). The individuals known as Bevan (Kuji) and Pryce (Datastream Cowboy) have been implicated in an incident that allegedly posed a significant risk of instigating a global conflict, commonly referred to as a third world war.

In addition, this perilous situation arose as a result of their unauthorized dissemination of classified KARI research materials into the computer systems utilized by the United States military. Bevan asserts his intention to substantiate a UFO conspiracy idea, and the BBC reports that his situation exhibits similarities to that of Gary McKinnon. Regardless of the presence of malicious intent, Bevan and Pryce's research showed the vulnerability of military networks.

6. Jeanson James Ancheta

Jeanson James Ancheta
The term "Jeanson" refers to a specific individual or concept that requires further clarification, or James Ancheta exhibited a lack of inclination towards engaging in activities such as hacking
systems to obtain credit card data or disrupting networks with the intention of promoting social justice. On the other hand, Ancheta exhibited a sense of inquisitiveness regarding the utilization of bots, which are computer programs designed to infiltrate and, afterward, manipulate computer systems.
By using a collection of extensive "botnets," the individual successfully infiltrated over 400,000 computer systems in the year 2005. As reported by ArsTechnica, the individual subsequently leased these workstations to advertising firms and received compensation for the direct installation of bots or adware on targeted systems. Ancheta received a prison sentence of 57 months. This marked the inaugural instance in which an individual engaging in the utilization of botnet technology was incarcerated.

7. Michael Calce

Michael Calce
In the month of February 2000, an individual named Michael Calce, who was 15 years old at the time and commonly referred to as "Mafiaboy," successfully identified a method to gain control over networks consisting of computers belonging to several universities. Utilizing their collective resources, he employed strategies to disrupt Yahoo, which was the leading search engine during that period. In a span of seven days, the individual successfully executed a distributed denial-of-service (DDoS) attack, resulting in the disruption of operations for prominent corporations such as Dell, eBay, CNN, and Amazon.
Calce's wake-up call proved to be quite disconcerting for investors in cybercrime and advocates of the internet. The emergence of cybercrime legislation swiftly assumed paramount importance among governmental circles following Calce's attack, a development that can be characterized as anything but an overstatement.

8.Kevin Poulsen

Poulsen was promptly apprehended and subsequently subjected to a three-year prohibition on computer usage. Subsequently, he transitioned to white hat hacking and journalism, whereby he focuses on authoring articles pertaining to cyber security and web-related socio-political issues. His written works have been published on reputable platforms such as Wired, The Daily Beast, and his personal site, Threat Level. Paulson collaborated with prominent hackers to engage in several initiatives focused on social justice and the promotion of unrestricted access to information. One noteworthy collaboration involved the development of the open-source software SecureDrop, originally referred to as DeadDrop, in conjunction with Adam Swartz and Jim Dolan. Then, Poulsen relinquished control of the platform, thereby facilitating the establishment of a secure communication channel between journalists and sources, which was then entrusted to the Freedom of Press Foundation.

9. Jonathan James

Under the pseudonym comrade, Jonathan James illicitly gained unauthorized access to the
computer systems of multiple corporations. Furthermore, it is noteworthy to mention that James was a mere 15 years old throughout that period. During an interview with PC Mag, James said that his creative process was partially influenced by the literary work titled The Cuckoo's Egg, which chronicles the pursuit of a computer hacker during the 1980s.

In the year 2000, James was apprehended and subsequently received a six-month period of confinement within his residence, commonly referred to as house arrest. Additionally, he was subjected to a prohibition on engaging in recreational internet activities. Nevertheless, his incarceration for a period of six months was a direct consequence of a probation breach. In 2007, TJX, a retail establishment, experienced a security breach resulting in the unauthorized access and compromising of several customers' personal information.

10. ASTRA

This particular hacker
distinguishes himself from the remaining individuals on this roster by virtue of his perpetual anonymity in the public domain. Nevertheless, the Daily Mail has provided several details regarding ASTRA. Specifically, it was in 2008 when he was caught by law enforcement officials, and during that period, he was recognized as a Greek mathematician who was 58 years old. Allegedly, he engaged in unauthorized access to the Dassault Group's systems over a period of around five years.

During that period, the individual illicitly acquired state-of-the-art weaponry technology software and data, thereafter engaging in the sale of those materials to a total of 250 individuals across various global locations. The reason behind the non-disclosure of his full identity remains unknown; nonetheless, it is noteworthy that the term 'ASTRA' originates from Sanskrit and denotes a ‘weapon.’

Wrapping Up Certain prominent hackers had the intention of fostering positive societal change, while others sought to substantiate beliefs pertaining to unidentified flying objects (UFOs). Specific individuals desired financial gain, while others aspired to achieve recognition and renown. Each of these individuals had a significant part in the advancement of the internet and the field of cyber security.