Part 1.

https://cybernews.com/security/brief-history-of-cybersecurity-and-hacking/

**Where did the term “hacker” originate?**

The word “hacking” has been used to describe “cutting in a rough and violent way, often without aiming exactly” since around 1200 B.C., and it didn’t have any association with tech until midway through the 20th Century.

**“Hacking” was first used in relation to using technical know-how back in 1955** at a meeting of the Technical Model Railroad Club. In the meeting minutes, it was used to describe how members modified the functions of their high-tech train sets.

Throughout the 1960s, the term became broader to encompass the growing legions of computing enthusiasts. And by 1975, one of the accepted definitions of a hacker by [The Jargon File](http://www.catb.org/~esr/jargon/html/H/hacker.html) was, “A malicious meddler who tries to discover sensitive information by poking around. Hence password hacker, network hacker.” This was the first time the word was on record as being associated with cybercrime.

Nowadays, the term “hacker” can be used to describe any skilled computer programmer, although it’s **usually synonymous with “security hacker**." A security hacker uses technical knowledge of bugs or vulnerabilities to exploit weaknesses in computer systems to access data that they otherwise wouldn’t have permission to view. Security hacking is usually illegal and can result in hefty fines or even a prison sentence.

**Who was the first hacker in history?**

John Draper, also known as Captain Crunch, is often named as the first ever hacker. And rather than having lots of high-tech hacking tools at his disposal, he managed to do it all with a toy whistle from a cereal packet. Here’s how:

Back in the early 1970s, the largest computer network accessible to the general public was the telephone system. And at the time, telephones were managed by an automated system that used specific analogue frequencies to place calls. Draper managed to exploit this using a toy whistle that came free in boxes of Cap’n Crunch cereal (hence the nickname). He would use this to make free long distance and international calls. This technique was known as “Phreaking”.

**The first internet hacker**

One of the first internet hackers, and certainly the first to gain mainstream media attention, was Robert Morris back in 1989. His was the first “Denial of service” attack in history and it was caused by a worm Morris had developed at Cornell University the year before.

According to Morris, he didn’t intend to cause any harm, but rather to highlight security flaws. But unfortunately, due to a fault in the code, the worm replicated excessively, causing extensive damage that lasted for days.

Part 2.

https://www.sluiceartfair.com/2021/writing-helper/where-did-hacking-originate-from/

**How was hacking created?**

The very first hack came in 1878 when the phone company, Bell Telephone, was started. A group of teenage boys, hired to run the switchboards, would disconnect or misdirect calls. The first authentic computer hackers came in the 1960s. In the 1970s, the world was primed and ready for hackers.

**Where did the term hacking and cracking come from?**

The term started out at MIT in the 1950s. It originally meant to deal with a technical problem in a creative way without any negative connotations. By 1975, a jargon dictionary for computer programmers contained multiple definitions of the word with only one of them meaning a person who was up to no good.

**Why did people start hacking into computer systems?**

When hacking first originated, the urge to hack into computer systems was based purely on curiosity. Curiosity of what the system did, how the system could be used, HOW the system did what did, and WHY it did what it did.

Part 3.

<https://www.helpnetsecurity.com/2002/04/08/the-history-of-hacking/>

**The History Of Hacking**

Nowadays, different people have different views on the hacking scene. ….

It all began in the 1960s at MIT, origin of the term “hacker”, where extremely skilled individuals practiced hardcore programming in FORTRAN and other older languages. Some may ignorantly dub them “nerds” or “geeks” but these individuals were, by far, the most intelligent, individual, and intellectually advanced people who happen to be the pioneers and forefathers of the talented individuals that are today the true hackers. The true hackers amongst our societies have an unquenchable thirst for knowledge. Boredom is never an object of challenge for hackers. They have an almost anomalous ability to absorb, retain, and exert vast amounts of knowledge with regard to intricate details. In 1969, Bell Labs employee Ken Thompson invented UNIX and permanently changed the future of the computer industry. Then in the very early 1970s, Dennis Ritchie invented the computer programming language “C” which was specifically invented to be used with UNIX. Programmers ceased to use assembler, while developing an appreciation for the portability of “C.”

Hackers used to be viewed as people who sat locked in a room all day programming nonstop, hours on end. No one seemed to mind hackers back in the 1960s when this was the most widely excepted reputation. In fact, most people had no idea what hacking was. The term hacker was accepted as a positive label slapped onto computer gurus who could push computer systems beyond the defined limits. Hackers emerged out of the artificial intelligence labs at MIT in the 1960s. A network known as ARPANET was founded by the Department of Defense as a means to link government offices. In time, ARPANET evolved into what is today known as the Internet.

In the 1970s, “Captain Crunch” devised a way to make free long distance calls and groups of phone hackers, later dubbed “phreakers” emerged. Throughout the 1970s and halfway into the 1980s, XEROX’s Palo Alto Research Center (PARC) spit out fresh new innovations such as the laser printer and LANs.

During the early 1980s, the term “cyberspace” is coined from a novel called “Neuromancer.” A group called the “414s” is one of the earliest hacker groups to ever get raided by the FBI and they get charged with 60 computer intrusions. Usenets began to pop up around the nation at this time and hackers exchanged thoughts using their UNIX based machines. While all of this was going on, the Secret Service was granted jurisdiction over credit card and computer fraud. During the 1980s, hacking was not known amongst the masses as it is presently. To be a hacker was to be a part of a very exclusive and secluded group. The infamous hacker groups the “Legion of Doom,” based in the USA and the “Chaos Computer Club,” based in Germany, were founded and are still two of the most widely recognized and respected hacker groups ever founded. Another significant foundation is that of “2600: The Hacker Quarterly,” an old school hacker magazine or “zine.” 2600 Magazine still continues to play a role in today’s hacker community. As the end of the decade approached, Kevin Mitnick was arrested and sentenced to a year in prison on convictions of stealing software and damaging computers. In addition, federal officials raided Atlanta, where some members of the Legion of Doom were residing, at the time. The LOD, CCC, and 2600 Magazine have become known as old school hackers and are still widely respected and recognized.

During the 1990s, Kevin Mitnick is arrested after being tracked down by Tsutomu Shimomura. The trials of Kevin Mitnick were of the most publicized hacker trials in hacker history.

As hackers and time progressed, hackers found ways to exploit holes in operating systems of local and remote machines.

Hackers have developed methods to exploit security holes in various computer systems. As protocols become updated, hackers probe them on a neverending mission to make computing more secure. In fact, due to the tendency hackers have of exploiting society, there have been spinoff categories such as “cracking” which deals with cracking software, “phreaking” which deals with exploiting phone systems, and “social engineering” which is the practice of exploiting human resources. When hacking first originated, the urge to hack into computer systems was based purely on curiosity. Curiosity of what the system did, how the system could be used, HOW the system did what did, and WHY it did what it did.

... Hackers find and release the vulnerabilities in computer systems which, if not found, could remain secret and one day lead to the downfall of our increasingly computer dependant civilization. In a way, hackers are the regulators of electronic communication. Hackers come up with useful new computer systems and solutions to make life easier for all of humanity. Whether you know it or not, I know from personal experience that ANYBODY you know could very well lead an unexposed life as a hacker. Hackers live amongst us all. They work in all of our major corporations, as well as in many small companies. Some choose to use their skills and help our government, others choose to use their skills in a more malicious and negative way. If you look around you, ANY INDIVIDUAL you see is a potential hacker. Often, it’s the people who you would suspect the least that are the hackers in our society.

….

Currently, we see the commercialization of hacking. If you were to take a trip to a respectable bookstore with a good selection of books, you would find books with flat out hacking techniques. Whether these techniques can truly be classified as hacking by the classic definition of hacking is debatable. They claim to teach you hacking methods, how to become a hacker, and supposedly reveal hacker tricks to the common man.

Another common misconception is that people who distribute and deal with illegal software, which is commonly known as “warez” are hackers. “Warez kings,” as they are commonly known, are not necessarily hackers, however that doesn’t mean that they are NOT hackers. You cannot determine the intellectual content of people by what they say or have. Moreover, hackers are not people who go around using programs in Windows such as “WinNuke” and various ICMP bombers and other miscellaneous Denial of Service programs designed to crash remote party’s machines. Hackers don’t distribute remote administration tools and use them as trojan horse viruses to wreak havoc on the general public and make other people’s lives miserable. Real hackers want to know as much as they can and are more helpful than wreckless. While it is true that there ARE hackers that DO commit malicious acts against users, they are not to be used as a model of the norm of hackers.

Part 4.

 https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/

Nowadays, the word “hacker” carries an overwhelmingly negative connotation, conjuring up images of digital thieves intent on stealing identities and letting disruptive viruses loose into cyberspace.

It wasn’t always that way. In fact, computer hackers were originally viewed by society as technology enthusiasts who wanted nothing more than to optimize, customize and tinker. It wasn’t until decades later – with the birth of viruses and cyber crime – that traditional hackers got lumped together with those of malicious intent and the public vilification of hacking began.

Curious as to how this evolution came to be? We were too, which is why we decided to go digging into the history of hacking.

1960S

Interestingly, the term “hack” did not originate from computers. Rather, it originated with [MIT’s Tech Model Railroad Club](http://catb.org/esr/writings/hacker-history/hacker-history-3.html) way back in 1961 when club members hacked their high-tech train sets in order to modify their functions. They later [moved on from toy trains to computers](http://www.campusactivism.org/html-resource/hackers/section4.html), using the elusive and expensive IBM 704’s at MIT to innovate, explore, create new paradigms, and try to expand the tasks that computers could accomplish.

These MIT students – along with other early hackers – were interested only in exploring, improving and testing the limits of existing programs. In some cases, these hacks even produced programs that were considerably better than the pre-existing ones, as was the case with Dennis Ritchie’s and Keith Thompson’s [UNIX operating system](http://www.unix.org/what_is_unix/history_timeline.html).

1970S

While computer hacking continued to flourish in the 1970s, the decade also gave way to a new type of hacker: one that toyed with telephone systems. Dubbed “phreakers,” phone hackers, such as the infamous John Draper, exploited operational characteristics in the telephone switching network, which had recently gone completely electronic.

Draper legendarily discovered that a toy whistle found in Cap’n Crunch cereal produced the exact tone necessary – 2600 hertz – to indicate to long lines that a line was ready and available to route a new call. This allowed him and other phreakers to dupe the network and make free long distance calls.

The phreaker subculture not only gave way to influential hackers like Draper but also to digital visionaries, as well. Before they went on to found one of the most successful computer companies in the world, [Steve Wozniak and Steve Jobs were, in fact, humble phone phreakers](http://www.esquire.com/news-politics/a38878/steve-jobs-steve-wozniak-blue-box-phone-phreaking/).

1980S

The 1980s was a watershed decade in the history of hacking, as it marked the introduction of turnkey personal computers to the general public. No longer limited to businesses and prestigious universities, computers were available for everyone to use for their own purposes – whatever that may be. Unsurprisingly, the wide availability of personal PCs led to a rapid increase in hackers.

It was not the only big change to occur in the hacking community. While there were still a large number of hackers interested primarily in tinkering with operating systems, a new breed emerged that was more concerned with personal gain. Instead of using their technological know-how for improving computers, they used it for criminal activities, including pirating software, creating viruses and breaking into systems to steal sensitive information.

It did not take the law long to respond. The emergence of cyber criminals was swiftly met in 1986 with the first legislation related to hacking, the [Federal Computer Fraud and Abuse Act](https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_%28CFAA%29).

Meanwhile, this was also the time that the idea of hackers being digital savants capable of doing both great and terrible things entered popular culture. A number of books and films were made that popularized the idea, mostly notably the 1983 flick [War Games](http://www.imdb.com/title/tt0086567/) in which a suburban teenager finds a backdoor in a military central computer and nearly starts World War III.

1990S

Riding on the coattails of the big changes that occurred in the 1980s, the 1990s were when hacking really began to achieve notoriety. The term hacker was tarnished by an ever increasing number of cyber crimes perpetrated by [“crackers”](http://www.techrepublic.com/blog/it-security/hacker-vs-cracker/) (or malicious hackers) and the high-profile arrests that followed.

[Kevin Mitnick, Kevin Poulsen, Robert Morris and Vladimir Levin](https://www.bestvpn.com/notorious-cyber-criminals/) were some of the more notable crackers to come out of the decade, having been arrested and convicted for the likes of stealing propriety software from big name corporations, duping radio stations to win luxury cars, launching the first computer worm, and leading the first digital bank heist.

The once close-knit hacking community also saw its breakdown in this decade. In an effort to crack down on computer crime, the Secret Service launched sting investigations, conducted early morning raids and arrested a number of hackers. Trying to avoid conviction, members in the hacking community began to inform on each other in exchange for immunity.

2000S

Ethical hackers continued to see their good name dragged in the dirt in the 2000s as attacks launched by malicious hackers dominated the headlines.

New and dangerous types of hacks emerged that victimized government entities and prominent businesses. Microsoft, eBay, Yahoo! and Amazon were among those taken down in massive [denial-of-service attacks](https://www.tripwire.com/state-of-security/security-data-protection/knowing-is-half-the-battle-building-a-deeper-understanding-of-ddos-attacks/), while the Department of Defense and International Space Station had its systems breached by a [15-year-old boy](https://en.wikipedia.org/wiki/Jonathan_James).

2010S

The world now firmly in the digital age, the hacking community has become more sophisticated, complicated and complex than ever.

Lone wolf hackers and small hacking groups still exist in every corner of the internet, either optimizing software or launching [ransomware](https://www.tripwire.com/state-of-security/security-awareness/how-why-is-ransomware/) and Wi-Fi attacks depending on their hat. That said, it’s “hacktivist” groups, such as Anonymous, that have taken center stage in this decade, releasing highly classified documents, exposing government secrets and leading vigilante digital crusades in the name of defending the public from being harmed, exploited, or withheld information.

In reaction to both hacktivists and cyber criminals, government entities and big corporations are scrambling to improve security while computer giants work hard to tweak their systems. However, while cyber security experts continue to be recruited, systems upgraded and technology innovated, hackers—good and bad—consistently and unsurprisingly stay one step ahead.

Part 5.

<https://searchsecurity.techtarget.com/definition/hacker>

**What is a hacker?**

A hacker is an individual who uses computer, networking or other skills to overcome a technical problem. The term also may refer to anyone who uses their abilities to gain unauthorized access to systems or networks in order to commit crimes. A hacker may, for example, steal information to hurt people via identity theft or [bring down a system](https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know) and, often, hold it hostage in order to collect a ransom.

The term hacker has historically been a divisive one, sometimes being used as a term of admiration for individuals who exhibit a high degree of skill and creativity in their approach to technical problems. However, the term is also commonly applied to individuals who use this skill for illegal or unethical purposes.

Hacker was first used in the 1960s to describe a programmer or an individual who, in an era of highly constrained computer capabilities, could increase the efficiency of computer code in a way that removed, or hacked, excess machine code instructions from a program. It has evolved over the years to refer to someone with an advanced understanding of computers, networking, programming or hardware.

**How does hacking work?**

Hackers use technical skills to [exploit cybersecurity defenses](https://searchsecurity.techtarget.com/feature/How-to-fix-the-top-5-cybersecurity-vulnerabilities). Ethical hackers test for cybersecurity vulnerabilities and may take up [hacking as a profession](https://whatis.techtarget.com/feature/A-guide-for-how-to-become-an-ethical-hacker) -- for example, a penetration tester (pen tester) -- or as a hobby. The end goal is often to gain unauthorized access to computers, networks, computing systems, mobile devices or internet of things systems. Many professional hackers use their skills to determine security holes in enterprise systems and then advise where companies should boost their security defenses to keep threat actors out.

Results can also be deleterious: Malicious hackers may steal login credentials, financial information and other types of sensitive information.

Many hackers aim to exploit either technical or social weaknesses to breach defenses. Technical weaknesses may include vulnerabilities in software or other exploitable weak spots. To exploit social weaknesses, hackers may attempt to manipulate social outcomes through false pretenses, such as impersonating a co-worker or other individual to gain financial or login information. Hackers may also use their technical skills to install dangerous malware, steal or destroy data, or disrupt an organization's services.

Hackers of all types participate in forums to exchange hacking information and tradecraft. There are numerous hacker forums where ethical hackers can discuss or ask questions about hacking. Many of these hacker forums offer technical guides with step-by-step instructions on hacking.

In contrast, forums and marketplaces serving threat actors or criminal hackers are often hosted on the [dark web](https://whatis.techtarget.com/definition/dark-web) and provide an outlet for offering, trading and soliciting illegal hacking services.

Criminal hackers, who sometimes lack technical skills, often use scripts and other specifically designed software programs to break into corporate networks. This software may manipulate network data to gather intelligence about the workings of the target system. These scripts can be found posted on the internet for anyone, usually entry-level hackers, to use. Hackers with limited skills are sometimes called [script kiddies](https://searchsecurity.techtarget.com/definition/script-kiddy-or-script-kiddie), referring to their need to use malicious scripts and their inability to create their own code. Advanced malicious hackers might study these scripts and then modify them to develop new methods.