**Hacker (computer security)**

From Wikipedia, the free encyclopedia

Jump to: [navigation](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#mw-head), [search](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#p-search)

[Page move-protected](http://en.wikipedia.org/wiki/Wikipedia:Protection_policy#move)

|  |
| --- |
| This article is part of a series on |
| **Computer hacking** |
| [**History**](http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history) |
| * [Phreaking](http://en.wikipedia.org/wiki/Phreaking) * [Cryptovirology](http://en.wikipedia.org/wiki/Cryptovirology) |
| **Hacker ethic** |
| * [Hacker Manifesto](http://en.wikipedia.org/wiki/Hacker_Manifesto) * [Black hat](http://en.wikipedia.org/wiki/Black_hat_%28computer_security%29) * [Grey hat](http://en.wikipedia.org/wiki/Grey_hat) * [White hat](http://en.wikipedia.org/wiki/White_hat_%28computer_security%29) * [Black Hat Briefings](http://en.wikipedia.org/wiki/Black_Hat_Briefings) * [DEF CON](http://en.wikipedia.org/wiki/DEF_CON) |
| [**Computer crime**](http://en.wikipedia.org/wiki/Computer_crime) |
| * [Crimeware](http://en.wikipedia.org/wiki/Crimeware) * [List of computer criminals](http://en.wikipedia.org/wiki/List_of_computer_criminals) * [Script kiddie](http://en.wikipedia.org/wiki/Script_kiddie) |
| [**Hacking tools**](http://en.wikipedia.org/wiki/Hacking_tool) |
| * [Vulnerability](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29) * [Exploit](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29) * [Payload](http://en.wikipedia.org/wiki/Payload_%28computing%29) |
| [**Malware**](http://en.wikipedia.org/wiki/Malware) |
| * [Rootkit](http://en.wikipedia.org/wiki/Rootkit) * [Backdoor](http://en.wikipedia.org/wiki/Backdoor_%28computing%29) * [Trojan horse](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29) * [Virus](http://en.wikipedia.org/wiki/Computer_virus) * [Worm](http://en.wikipedia.org/wiki/Computer_worm) * [Spyware](http://en.wikipedia.org/wiki/Spyware) * [Botnet](http://en.wikipedia.org/wiki/Botnet) * [Keystroke logging](http://en.wikipedia.org/wiki/Keystroke_logging) * [Antivirus software](http://en.wikipedia.org/wiki/Antivirus_software) * [Firewall](http://en.wikipedia.org/wiki/Firewall_%28computing%29) * [HIDS](http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system) |
| [**Computer security**](http://en.wikipedia.org/wiki/Computer_security) |
| * [Computer insecurity](http://en.wikipedia.org/wiki/Computer_insecurity) * [Application security](http://en.wikipedia.org/wiki/Application_security) * [Network security](http://en.wikipedia.org/wiki/Network_security) |
| **Groups** |
| * [Hacker group](http://en.wikipedia.org/wiki/Hacker_group) |
| * [v](http://en.wikipedia.org/wiki/Template:Computer_hacking) * [t](http://en.wikipedia.org/wiki/Template_talk:Computer_hacking) * [e](http://en.wikipedia.org/w/index.php?title=Template:Computer_hacking&action=edit) |

In the computer security context, a **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge.[[1]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-crackdown-1) The subculture that has evolved around hackers is often referred to as the computer underground and is now a known [community](http://en.wikipedia.org/wiki/Community).[[2]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-2) While other uses of the word hacker exist that are not related to computer security, such as referring to someone with an advanced understanding of computers and computer networks,[[3]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-3) they are rarely used in mainstream context.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] They are subject to the long standing [hacker definition controversy](http://en.wikipedia.org/wiki/Hacker_definition_controversy) about the true meaning of the term [hacker](http://en.wikipedia.org/wiki/Hacker_%28term%29). In this controversy, the term hacker is reclaimed by [computer programmers](http://en.wikipedia.org/wiki/Hacker_%28programmer_subculture%29) who argue that someone breaking into computers is better called a **cracker**,[[4]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-4) not making a difference between computer criminals ([black hats](http://en.wikipedia.org/wiki/Black_hat_hacking)) and computer security experts ([white hats](http://en.wikipedia.org/wiki/White_hats)).[[5]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-5) Some white hat hackers claim that they also deserve the title hacker, and that only black hats should be called crackers.

|  |
| --- |
| **Contents**   * [1 History](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#History) * [2 Classifications](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Classifications)   + [2.1 White hat](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#White_hat)   + [2.2 Black hat](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Black_hat)   + [2.3 Grey hat](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Grey_hat)   + [2.4 Elite hacker](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Elite_hacker)   + [2.5 Script kiddie](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Script_kiddie)   + [2.6 Neophyte](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Neophyte)   + [2.7 Blue hat](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Blue_hat)   + [2.8 Hacktivist](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Hacktivist)   + [2.9 Nation state](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Nation_state)   + [2.10 Organized criminal gangs](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Organized_criminal_gangs)   + [2.11 Bots](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Bots) * [3 Attacks](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Attacks)   + [3.1 Security exploits](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Security_exploits)   + [3.2 Techniques](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Techniques) * [4 Notable intruders and criminal hackers](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Notable_intruders_and_criminal_hackers) * [5 Notable security hackers](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Notable_security_hackers) * [6 Customs](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Customs)   + [6.1 Hacker groups and conventions](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Hacker_groups_and_conventions) * [7 Hacking and the law](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Hacking_and_the_law)   + [7.1 Netherlands](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Netherlands) * [8 Hacking and the media](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Hacking_and_the_media)   + [8.1 Hacker magazines](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Hacker_magazines)   + [8.2 Hackers in fiction](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Hackers_in_fiction)   + [8.3 Non-fiction books](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Non-fiction_books)   + [8.4 Fiction books](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Fiction_books) * [9 See also](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#See_also) * [10 References](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#References) * [11 Related literature](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#Related_literature) * [12 External links](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#External_links) |

**History**

Further information: [Timeline of computer security hacker history](http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history)

[Bruce Sterling](http://en.wikipedia.org/wiki/Bruce_Sterling) traces part of the roots of the computer underground to the [Yippies](http://en.wikipedia.org/wiki/Yippies), a 1960s counterculture movement which published the *Technological Assistance Program* (TAP) newsletter.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] *TAP* was a [*phone phreaking*](http://en.wikipedia.org/wiki/Phreaking) newsletter that taught the techniques necessary for the unauthorized exploration of the phone network. Many people from the phreaking community are also active in the hacking community even today, and vice versa.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Classifications**

Several subgroups of the computer underground with different attitudes use different terms to demarcate themselves from each other, or try to exclude some specific group with which they do not agree. [Eric S. Raymond](http://en.wikipedia.org/wiki/Eric_S._Raymond) (author of [The New Hacker's Dictionary](http://en.wikipedia.org/wiki/Jargon_File)) advocates that members of the computer underground should be called crackers. Yet, those people see themselves as hackers and even try to include the views of Raymond in what they see as one wider hacker culture, a view harshly rejected by Raymond himself. Instead of a hacker/cracker dichotomy, they give more emphasis to a spectrum of different categories, such as [white hat](http://en.wikipedia.org/wiki/White_hat_%28computer_security%29), [grey hat](http://en.wikipedia.org/wiki/Grey_hat), [black hat](http://en.wikipedia.org/wiki/Black_hat_hacking) and [script kiddie](http://en.wikipedia.org/wiki/Script_kiddie). In contrast to Raymond, they usually reserve the term cracker for more malicious activity. According to (Clifford R.D. 2006) a cracker or cracking is to "gain unauthorized access to a computer in order to commit another crime such as destroying information contained in that system".[[6]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-Cybercrime:The_Investigation.2C_Prosecution_and_Defense_of_a_Computer-Related_Crime-6) These subgroups may also be defined by the legal status of their activities.[[7]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-hacker_hats-7)

**White hat**

A [white hat hacker](http://en.wikipedia.org/wiki/White_hat_%28computer_security%29) breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an [ethical hacker](http://en.wikipedia.org/wiki/Ethical_hacker). This classification also includes individuals who perform [penetration tests](http://en.wikipedia.org/wiki/Penetration_testing) and [vulnerability assessments](http://en.wikipedia.org/wiki/Vulnerability_assessment) within a contractual agreement. The EC-Council,[[8]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-8) also known as the International Council of Electronic Commerce Consultants, is one of those organisations that have developed certifications, courseware, classes, and online training covering the diverse arena of Ethical Hacking.[[7]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-hacker_hats-7)

**Black hat**

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005).[[9]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-Moore2005-9) Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal".[[10]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-moore2006-10) Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network. They choose their targets using a two-pronged process known as the "pre-hacking stage".

**Part 1: Targeting**

The hacker determines what network to break into during this phase. The target may be of particular interest to the hacker, either politically or personally, or it may be picked at random. Next, they will [port](http://en.wikipedia.org/wiki/Port_%28computer_networking%29) scan a network to determine if it is vulnerable to attacks, which is just testing all ports on a host machine for a response. Open ports—those that do respond—will allow a hacker to access the system.

**Part 2: Research and Information Gathering**

It is in this stage that the hacker will visit or contact the target in some way in hopes of finding out vital information that will help them access the system. The main way that hackers get desired results from this stage is from "social engineering", which will be explained below. Aside from social engineering, hackers can also use a technique called "dumpster diving". Dumpster diving is when a hacker will literally search through users' garbage in hopes of finding documents that have been thrown away, which may contain information a hacker can use directly or indirectly, to help them gain access to a network.

**Part 3: Finishing The Attack**

This is the stage when the hacker will invade the primary target that he/she was planning to attack or steal from. Many "hackers" will be caught after this point, lured in or grabbed by any data also known as a [honeypot](http://en.wikipedia.org/wiki/Honeypot_%28computing%29) (a trap set up by computer security personnel).

**Grey hat**

Main article: [Grey hat](http://en.wikipedia.org/wiki/Grey_hat)

A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked, for example. Then they may offer to repair their system for a small fee.[[10]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-moore2006-10)

**Elite hacker**

A [social status](http://en.wikipedia.org/wiki/Achieved_status) among hackers, *elite* is used to describe the most skilled. Newly discovered [exploits](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29) will circulate among these hackers. Elite [groups](http://en.wikipedia.org/wiki/Hacker_group) such as [Masters of Deception](http://en.wikipedia.org/wiki/Masters_of_Deception) conferred a kind of credibility on their members.[[11]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-thomas2002-11)

**Script kiddie**

A [script kiddie](http://en.wikipedia.org/wiki/Script_kiddie) (or skiddie) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept—hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature).[[12]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-Andress_10-12)

**Neophyte**

A neophyte, "[n00b](http://en.wikipedia.org/wiki/N00b)", or "[newbie](http://en.wikipedia.org/wiki/Newbie)" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology, and hacking.[[10]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-moore2006-10)

**Blue hat**

A [blue hat](http://en.wikipedia.org/wiki/BlueHat) hacker is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed. [Microsoft](http://en.wikipedia.org/wiki/Microsoft) also uses the term [BlueHat](http://www.microsoft.com/technet/security/bluehat/default.mspx) to represent a series of security briefing events.[[13]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-13)[[14]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-14)[[15]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-15)

**Hacktivist**

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most [hacktivism](http://en.wikipedia.org/wiki/Hacktivism) involves website defacement or [denial-of-service attacks](http://en.wikipedia.org/wiki/Denial-of-service_attack).

**Nation state**

Intelligence agencies and cyberwarfare operatives of nation states.[[16]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-GISEC-16)

**Organized criminal gangs**

Criminal activity carried on for profit.[[16]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-GISEC-16)

**Bots**

Bots are automated software tools, some freeware, that are available for the use of any type of hacker.[[16]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-GISEC-16)

**Attacks**

Main article: [Computer insecurity](http://en.wikipedia.org/wiki/Computer_insecurity)

|  |
| --- |
| [**Computer security**](http://en.wikipedia.org/wiki/Computer_security) |
| * [Secure operating systems](http://en.wikipedia.org/wiki/Security-focused_operating_system) * [Security by design](http://en.wikipedia.org/wiki/Security_by_design) * [Secure coding](http://en.wikipedia.org/wiki/Secure_coding) |
| [**Computer insecurity**](http://en.wikipedia.org/wiki/Computer_insecurity) |
| * [Vulnerability](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29)   + [Eavesdropping](http://en.wikipedia.org/wiki/Eavesdropping) * [Exploits](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29)   + [Trojans](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29)   + [Viruses](http://en.wikipedia.org/wiki/Computer_virus) and [worms](http://en.wikipedia.org/wiki/Computer_worm)   + [Denial of service](http://en.wikipedia.org/wiki/Denial_of_service) * [Payloads](http://en.wikipedia.org/wiki/Payload_%28computing%29)   + [Rootkits](http://en.wikipedia.org/wiki/Rootkit)   + [Keyloggers](http://en.wikipedia.org/wiki/Keylogger) |
| * [v](http://en.wikipedia.org/wiki/Template:Computer_security) * [t](http://en.wikipedia.org/wiki/Template_talk:Computer_security) * [e](http://en.wikipedia.org/w/index.php?title=Template:Computer_security&action=edit) |

A typical approach in an attack on Internet-connected system is:

1. [Network enumeration](http://en.wikipedia.org/wiki/Network_enumeration): Discovering information about the intended target.
2. [Vulnerability analysis](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29): Identifying potential ways of attack.
3. [Exploitation](http://en.wikipedia.org/wiki/Exploitation): Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.[[17]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-17)

In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts.

**Security exploits**

Main article: [Exploit (computer security)](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29)

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are [SQL injection](http://en.wikipedia.org/wiki/SQL_injection), [Cross Site Scripting](http://en.wikipedia.org/wiki/Cross_Site_Scripting) and [Cross Site Request Forgery](http://en.wikipedia.org/wiki/Cross_Site_Request_Forgery) which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through [FTP](http://en.wikipedia.org/wiki/FTP), [HTTP](http://en.wikipedia.org/wiki/HTTP), [PHP](http://en.wikipedia.org/wiki/PHP), [SSH](http://en.wikipedia.org/wiki/Secure_Shell), [Telnet](http://en.wikipedia.org/wiki/Telnet) and some web-pages. These are very common in website/domain hacking.

**Techniques**

|  |  |
| --- | --- |
| [Question book-new.svg](http://en.wikipedia.org/wiki/File:Question_book-new.svg) | This section **does not** [**cite**](http://en.wikipedia.org/wiki/Wikipedia:Citing_sources) **any** [**references or sources**](http://en.wikipedia.org/wiki/Wikipedia:Verifiability). Please help improve this section by [adding citations to reliable sources](http://en.wikipedia.org/wiki/Help:Introduction_to_referencing/1). Unsourced material may be challenged and [removed](http://en.wikipedia.org/wiki/Wikipedia:Verifiability#Burden_of_evidence). *(August 2011)* |

Vulnerability scanner

Main article: [Vulnerability scanner](http://en.wikipedia.org/wiki/Vulnerability_scanner)

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use [port scanners](http://en.wikipedia.org/wiki/Port_scanner). These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Note that [firewalls](http://en.wikipedia.org/wiki/Firewall_%28networking%29) defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented.)

Password cracking

Main article: [Password cracking](http://en.wikipedia.org/wiki/Password_cracking)

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Packet sniffer

Main article: [Packet sniffer](http://en.wikipedia.org/wiki/Packet_sniffer)

A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack (Phishing)

Main article: [Spoofing attack](http://en.wikipedia.org/wiki/Spoofing_attack)

A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.

Rootkit

Main article: [Rootkit](http://en.wikipedia.org/wiki/Rootkit)

A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at [process tables](http://en.wikipedia.org/wiki/Process_table).

Social engineering

Main article: [Social engineering (computer security)](http://en.wikipedia.org/wiki/Social_engineering_%28computer_security%29)

When a hacker, typically a black hat, is in the second stage of the targeting process, he or she will typically use some social engineering tactics to get enough information to access the network. A common practice for hackers who use this technique, is to contact the system administrator and play the role of a user who cannot get access to his or her system. Hackers who use this technique have to be quite savvy and choose the words they use carefully, in order to trick the system administrator into giving them information. In some cases only an employed help desk user will answer the phone and they are generally easy to trick. Another typical hacker approach is for the hacker to act like a very angry supervisor and when the his/her authority is questioned they will threaten the help desk user with their job. Social engineering is very effective because users are the most vulnerable part of an organization. All the security devices and programs in the world won't keep an organization safe if an employee gives away a password. Black hat hackers take advantage of this fact. Social engineering can also be broken down into four sub-groups. These are intimidation, helpfulness, technical, and name-dropping.

* ***Intimidation*** As stated above, with the angry supervisor, the hacker attacks the person who answers the phone with threats to their job. Many people at this point will accept that the hacker is a supervisor and give them the needed information.
* ***Helpfulness*** Opposite to intimidation, helpfulness is taking advantage of a person's natural instinct to help someone with a problem. The hacker will not get angry and instead act very distressed and concerned. The help desk is the most vulnerable to this type of social engineering, because it generally has the authority to change or reset passwords, which is exactly what the hacker needs.
* ***Name-dropping*** Simply put, the hacker uses the names of advanced users as "key words", and gets the person who answers the phone to believe that they are part of the company because of this. Some information, like web page ownership, can be obtained easily on the web. Other information such as president and vice president names might have to be obtained via dumpster diving.
* ***Technical*** Using technology is also a great way to get information. A hacker can send a fax or an email to a legitimate user in hopes to get a response containing vital information. Many times the hacker will act like he/she is involved with law enforcement and needs certain data for record keeping purposes or investigations.

Trojan horses

Main article: [Trojan horse (computing)](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29)

A Trojan horse is a program which seems to be doing one thing, but is actually doing another. A trojan horse can be used to set up a [back door](http://en.wikipedia.org/wiki/Backdoor_%28computing%29) in a computer system such that the intruder can gain access later. (The name refers to the [horse](http://en.wikipedia.org/wiki/Trojan_Horse) from the [Trojan War](http://en.wikipedia.org/wiki/Trojan_War), with the conceptually similar function of deceiving defenders into bringing an intruder inside.)

Viruses

Main article: [Computer virus](http://en.wikipedia.org/wiki/Computer_virus)

A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus behaves in a way similar to a [biological virus](http://en.wikipedia.org/wiki/Virus), which spreads by inserting itself into living cells.

While some are harmless or mere hoaxes, most computer viruses are considered malicious.

Worms

Main article: [Computer worm](http://en.wikipedia.org/wiki/Computer_worm)

Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing program. Many people conflate the terms "virus" and "worm", using them both to describe any self-propagating program.

Key loggers

Main article: [Keystroke logging](http://en.wikipedia.org/wiki/Keystroke_logging)

A key logger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. Some key loggers use virus-, trojan-, and rootkit-like methods to remain active and hidden. However, some key loggers are used in legitimate ways and sometimes to even enhance computer security. As an example, a business might have a key logger on a computer used at a [point of sale](http://en.wikipedia.org/wiki/Point_of_sale) and data collected by the key logger could be used for catching employee fraud.

**Notable intruders and criminal hackers**

Main article: [List of convicted computer criminals](http://en.wikipedia.org/wiki/List_of_convicted_computer_criminals)

**Notable security hackers**

Main article: [List of hackers](http://en.wikipedia.org/wiki/List_of_hackers)

* [Jacob Appelbaum](http://en.wikipedia.org/wiki/Jacob_Appelbaum) is an Advocate, Security Researcher, and Developer for the [Tor](http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29) project. He speaks internationally for usage of Tor by human rights groups and others concerned about internet anonymity and censorship.
* [Albert Gonzalez](http://en.wikipedia.org/wiki/Albert_Gonzalez) sentenced to 20 years in prison.
* [Eric Corley](http://en.wikipedia.org/wiki/Eric_Gorden_Corley) (also known as [Emmanuel Goldstein](http://en.wikipedia.org/wiki/Emmanuel_Goldstein)) is the long standing publisher of [2600: The Hacker Quarterly](http://en.wikipedia.org/wiki/2600_The_Hacker_Quarterly). He is also the founder of the [H.O.P.E.](http://en.wikipedia.org/wiki/H.O.P.E.) conferences. He has been part of the hacker community since the late '70s.
* [Ed Cummings](http://en.wikipedia.org/wiki/Ed_Cummings) (also known as [Bernie S](http://en.wikipedia.org/wiki/Bernie_S)) is the long standing writer for [2600: The Hacker Quarterly](http://en.wikipedia.org/wiki/2600_The_Hacker_Quarterly). He set legal precedence after denial of both a bail hearing and a speedy trial in 1995. Bernie S was charged with possession of technology which could be used for fraudulent purposes.
* [Dan Kaminsky](http://en.wikipedia.org/wiki/Dan_Kaminsky) is a [DNS](http://en.wikipedia.org/wiki/Domain_Name_System) expert who exposed multiple flaws in the protocol and investigated Sony's rootkit security issues in 2005. He has spoken in front of the US Senate on technology issues.
* [Gordon Lyon](http://en.wikipedia.org/wiki/Gordon_Lyon), known by the handle Fyodor, authored the [Nmap Security Scanner](http://en.wikipedia.org/wiki/Nmap) as well as many network security books and web sites. He is a founding member of the [Honeynet Project](http://en.wikipedia.org/wiki/Honeynet_Project) and Vice President of [Computer Professionals for Social Responsibility](http://en.wikipedia.org/wiki/Computer_Professionals_for_Social_Responsibility).
* [Gary McKinnon](http://en.wikipedia.org/wiki/Gary_McKinnon) is a Scottish hacker facing [extradition](http://en.wikipedia.org/wiki/Extradition) to the [United States](http://en.wikipedia.org/wiki/United_States) to face charges of perpetrating what has been described as a travesty of justice with many in the UK "show a little bit of compassion" to rule sooner who also suffers from [Asperger syndrome](http://en.wikipedia.org/wiki/Asperger_syndrome).[[18]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-bbcprofile-18)
* [Kevin Mitnick](http://en.wikipedia.org/wiki/Kevin_Mitnick) is a computer security consultant and author, formerly the most wanted computer criminal in [United States](http://en.wikipedia.org/wiki/United_States) history.[[19]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-19)
* [Rafael Núñez](http://en.wikipedia.org/wiki/Rafael_N%C3%BA%C3%B1ez_%28hacker%29) aka RaFa was a notorious most wanted hacker by the [FBI](http://en.wikipedia.org/wiki/FBI) since 2001.
* [Meredith L. Patterson](http://en.wikipedia.org/wiki/Meredith_L._Patterson) a well known technologist and [biohacker](http://en.wikipedia.org/wiki/Biohacker) who has presented research with [Dan Kamisky](http://en.wikipedia.org/w/index.php?title=Dan_Kamisky&action=edit&redlink=1) and [Len Sassaman](http://en.wikipedia.org/wiki/Len_Sassaman) at many international security and hacker conferences.
* [Len Sassaman](http://en.wikipedia.org/wiki/Len_Sassaman) a Belgian computer programmer and technologist who was also a privacy advocate.
* [Solar Designer](http://en.wikipedia.org/wiki/Solar_Designer) is the pseudonym of the founder of the [Openwall Project](http://en.wikipedia.org/wiki/Openwall_Project).
* [Michał Zalewski](http://en.wikipedia.org/wiki/Micha%C5%82_Zalewski) (lcamtuf) is a prominent security researcher.

**Customs**

The computer underground[[1]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-crackdown-1) has produced its own slang and various forms of unusual alphabet use, for example [1337speak](http://en.wikipedia.org/wiki/Leet). Political attitude usually includes views for freedom of information, freedom of speech, a right for anonymity and most have a strong opposition against copyright.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] Writing programs and performing other activities to support these views is referred to as [hacktivism](http://en.wikipedia.org/wiki/Hacktivism). Some go as far as seeing illegal cracking ethically justified for this goal; a common form is [website defacement](http://en.wikipedia.org/wiki/Website_defacement). The computer underground is frequently compared to the Wild West.[[20]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-20) It is common among hackers to use aliases for the purpose of concealing identity, rather than revealing their real names.

**Hacker groups and conventions**

Main articles: [Hacker conference](http://en.wikipedia.org/wiki/Hacker_conference) and [Hacker group](http://en.wikipedia.org/wiki/Hacker_group)

The computer underground is supported by regular real-world gatherings called [hacker conventions](http://en.wikipedia.org/wiki/Hacker_convention) or "hacker cons". These draw many people every year including [SummerCon](http://en.wikipedia.org/wiki/SummerCon) (Summer), [DEF CON](http://en.wikipedia.org/wiki/DEF_CON), [HoHoCon](http://en.wikipedia.org/wiki/HoHoCon) (Christmas), ShmooCon (February), BlackHat, AthCon, Hacker Halted, and [H.O.P.E.](http://en.wikipedia.org/wiki/H.O.P.E.).[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]. Local Hackfest groups organize and compete to develop skills to send a team to a prominent convention to compete in group pentesting, exploit and forensics on a wider scale. In the early 1980s Hacker Groups became popular, Hacker groups provided access to information and resources, and a place to learn from other members. BBS systems like Utopias provided a platform for information sharing via dialup. Hackers could also gain credibility by being affiliated with an elite group.[[21]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-thomas-21)

**Hacking and the law**

**Netherlands**

* Article 138ab of [Wetboek van Strafrecht](http://en.wikipedia.org/wiki/Wetboek_van_Strafrecht) prohibits *computervredebreuk* which is defined as intruding an automated work or a part thereof with intention and against the law. Intrusion is defined as access by means of:
  + breaking through a [security](http://en.wikipedia.org/wiki/Computer_security);
  + by technical means;
  + by false signals or a false [key](http://en.wikipedia.org/wiki/Key_%28cryptography%29);
  + by disguising, which is using a stolen [username](http://en.wikipedia.org/wiki/Username) and [password](http://en.wikipedia.org/wiki/Password).

Maximum imprisonment is one year or a fine of the fourth category.[[22]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-22)[[23]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-23)

**Hacking and the media**

|  |  |
| --- | --- |
| http://upload.wikimedia.org/wikipedia/en/thumb/f/f2/Edit-clear.svg/40px-Edit-clear.svg.png | This section **is in a list format that may be better presented using** [**prose**](http://en.wikipedia.org/wiki/Wikipedia:Proseline)**.** You can help by converting this section to prose, if [appropriate](http://en.wikipedia.org/wiki/Wikipedia:Embedded_list). [Editing help](http://en.wikipedia.org/wiki/Help:Editing) is available. *(August 2008)* |

**Hacker magazines**

Main category: [Hacker magazines](http://en.wikipedia.org/wiki/Category:Hacker_magazines)

The most notable hacker-oriented magazine publications are [*Phrack*](http://en.wikipedia.org/wiki/Phrack), [*Hakin9*](http://en.wikipedia.org/wiki/Hakin9) and [*2600: The Hacker Quarterly*](http://en.wikipedia.org/wiki/2600:_The_Hacker_Quarterly). While the information contained in hacker magazines and [ezines](http://en.wikipedia.org/wiki/Ezine) was often outdated, they improved the reputations of those who contributed by documenting their successes.[[21]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-thomas-21)

**Hackers in fiction**

See also: [List of fictional hackers](http://en.wikipedia.org/wiki/List_of_fictional_hackers)

Hackers often show an interest in fictional [cyberpunk](http://en.wikipedia.org/wiki/Cyberpunk) and [cyberculture](http://en.wikipedia.org/wiki/Cyberculture) literature and movies. Absorption of [fictional](http://en.wikipedia.org/wiki/Fictional) [pseudonyms](http://en.wikipedia.org/wiki/Pseudonym), symbols, values, and [metaphors](http://en.wikipedia.org/wiki/Metaphor) from these fictional works is very common.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Books portraying hackers:

* The [cyberpunk](http://en.wikipedia.org/wiki/Cyberpunk) novels of [William Gibson](http://en.wikipedia.org/wiki/William_Gibson) — especially the [Sprawl trilogy](http://en.wikipedia.org/wiki/Sprawl_trilogy) — are very popular with hackers.[[24]](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_note-ntygibson-24)
* [*Hackers* (short stories)](http://en.wikipedia.org/wiki/Hackers_%28short_stories%29)
* *Helba* from the [.hack](http://en.wikipedia.org/wiki/.hack) manga and anime series.
* [*Little Brother*](http://en.wikipedia.org/wiki/Little_Brother_%28Cory_Doctorow_novel%29) by [Cory Doctorow](http://en.wikipedia.org/wiki/Cory_Doctorow)
* [*Merlin*](http://en.wikipedia.org/wiki/Merlin_of_Amber), the protagonist of the second series in [The Chronicles of Amber](http://en.wikipedia.org/wiki/The_Chronicles_of_Amber) by [Roger Zelazny](http://en.wikipedia.org/wiki/Roger_Zelazny) is a young immortal hacker-mage prince who has the ability to traverse shadow dimensions.
* Lisbeth Salander in [*The Girl with the Dragon Tattoo*](http://en.wikipedia.org/wiki/The_Girl_with_the_Dragon_Tattoo) by [Stieg Larsson](http://en.wikipedia.org/wiki/Stieg_Larsson)
* [*Snow Crash*](http://en.wikipedia.org/wiki/Snow_Crash)
* Alice from [Kami-sama no Memo-chō](http://en.wikipedia.org/wiki/Kami-sama_no_Memo-ch%C5%8D)

Films also portray hackers:

|  |  |  |
| --- | --- | --- |
| * [*Antitrust*](http://en.wikipedia.org/wiki/Antitrust_%28film%29) * [*Cypher*](http://en.wikipedia.org/wiki/Cypher_%28film%29) * [*Eagle Eye*](http://en.wikipedia.org/wiki/Eagle_Eye) * [*Enemy of the State*](http://en.wikipedia.org/wiki/Enemy_of_the_State_%28film%29) * [*Firewall*](http://en.wikipedia.org/wiki/Firewall_%28film%29) * [*Girl With The Dragon Tattoo*](http://en.wikipedia.org/wiki/Girl_With_The_Dragon_Tattoo) * [*Hackers*](http://en.wikipedia.org/wiki/Hackers_%28film%29) | * [*Live Free or Die Hard*](http://en.wikipedia.org/wiki/Live_Free_or_Die_Hard) * [*Pirates of Silicon Valley*](http://en.wikipedia.org/wiki/Pirates_of_Silicon_Valley) * [*Sneakers*](http://en.wikipedia.org/wiki/Sneakers_%281992_film%29) * [*Skyfall*](http://en.wikipedia.org/wiki/Skyfall) * [*Swordfish*](http://en.wikipedia.org/wiki/Swordfish_%28film%29) * [*Take Down*](http://en.wikipedia.org/wiki/Track_Down) * [*The Matrix* series](http://en.wikipedia.org/wiki/The_Matrix_Series) * [*The Net*](http://en.wikipedia.org/wiki/The_Net_%281995_film%29) | * [*The Net 2.0*](http://en.wikipedia.org/wiki/The_Net_2.0_%28film%29) * [*Tron*](http://en.wikipedia.org/wiki/Tron_%28film%29) * [*Tron Legacy*](http://en.wikipedia.org/wiki/Tron_Legacy_%28film%29) * [*Untraceable*](http://en.wikipedia.org/wiki/Untraceable) * [*WarGames*](http://en.wikipedia.org/wiki/WarGames) * [*Weird Science*](http://en.wikipedia.org/wiki/Weird_Science_%28film%29) |

**Non-fiction books**

* [*Hacking: The Art of Exploitation, Second Edition*](http://en.wikipedia.org/wiki/Hacking:_The_Art_of_Exploitation,_Second_Edition) by Jon Erickson
* [*The Hacker Crackdown*](http://en.wikipedia.org/wiki/The_Hacker_Crackdown)
* [*The Art of Intrusion*](http://en.wikipedia.org/wiki/The_Art_of_Intrusion) by Kevin D. Mitnick
* [*The Art of Deception*](http://en.wikipedia.org/wiki/The_Art_of_Deception) by Kevin D. Mitnick
* [*Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*](http://en.wikipedia.org/wiki/Ghost_in_the_Wires) by Kevin D. Mitnick
* [*The Hacker's Handbook*](http://en.wikipedia.org/wiki/The_Hacker%27s_Handbook)
* [*The Cuckoo's Egg*](http://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg) by Clifford Stoll
* [*Underground*](http://en.wikipedia.org/wiki/Underground_%28Suelette_Dreyfus_book%29) by Suelette Dreyfus
* *Stealing the Network: How to Own the Box, How to Own an Identity, and How to Own an Continent* by various authors

**Fiction books**

* [*Ender's Game*](http://en.wikipedia.org/wiki/Ender%27s_Game)
* [*Evil Genius (novel)*](http://en.wikipedia.org/wiki/Evil_Genius_%28novel%29)
* [*Neuromancer*](http://en.wikipedia.org/wiki/Neuromancer)
* [*Snow Crash*](http://en.wikipedia.org/wiki/Snow_Crash)

**See also**

|  |  |
| --- | --- |
| * [Black hat hacking](http://en.wikipedia.org/wiki/Black_hat_hacking) * [Computer crime](http://en.wikipedia.org/wiki/Computer_crime) * [Computer hacking](http://en.wikipedia.org/wiki/Category:Hacking_%28computer_security%29) * [Cyber spying](http://en.wikipedia.org/wiki/Cyber_spying) * [Cyber Storm Exercise](http://en.wikipedia.org/wiki/Cyber_Storm_Exercise) * [Cyber warfare](http://en.wikipedia.org/wiki/Cyber_warfare) * [Exploit (computer security)](http://en.wikipedia.org/wiki/Exploit_%28computer_security%29) * [Grey hat](http://en.wikipedia.org/wiki/Grey_hat) * [Hack value](http://en.wikipedia.org/wiki/Hack_value) * [Hacker (programmer subculture)](http://en.wikipedia.org/wiki/Hacker_%28programmer_subculture%29) * [Hacker Manifesto](http://en.wikipedia.org/wiki/Hacker_Manifesto) | * [Hacker (term)](http://en.wikipedia.org/wiki/Hacker_%28term%29) * [Hacktivism](http://en.wikipedia.org/wiki/Hacktivism) * [IT risk](http://en.wikipedia.org/wiki/IT_risk) * [List of notable hackers](http://en.wikipedia.org/wiki/List_of_notable_hackers) * [Mathematical beauty](http://en.wikipedia.org/wiki/Mathematical_beauty) * [Metasploit](http://en.wikipedia.org/wiki/Metasploit) * [Penetration test](http://en.wikipedia.org/wiki/Penetration_test) * [Technology assessment](http://en.wikipedia.org/wiki/Technology_assessment) * [Vulnerability (computing)](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29) * [White hat](http://en.wikipedia.org/wiki/White_hat_%28computer_security%29) * [Wireless hacking](http://en.wikipedia.org/wiki/Wireless_hacking) |

**References**

* Taylor, Paul A. (1999). *Hackers*. Routledge. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-415-18072-6](http://en.wikipedia.org/wiki/Special:BookSources/978-0-415-18072-6).
  1. ^ [***a***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-crackdown_1-0) [***b***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-crackdown_1-1) [Sterling, Bruce](http://en.wikipedia.org/wiki/Bruce_Sterling) (1993). "Part 2(d)". [*The Hacker Crackdown*](http://en.wikipedia.org/wiki/The_Hacker_Crackdown). McLean, Virginia: IndyPublish.com. p. 61. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [1-4043-0641-2](http://en.wikipedia.org/wiki/Special:BookSources/1-4043-0641-2).
  2. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-2) Blomquist, Brian (May 29, 1999). ["FBI's Web Site Socked as Hackers Target Feds"](http://archive.nypost.com/a/475198). *New York Post*.
  3. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-3) rfc 1983
  4. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-4) S. Raymond, Eric. ["Jargon File: Cracker"](http://catb.org/jargon/html/C/cracker.html). Retrieved 2010-05-08. "Coined ca. 1985 by hackers in defense against journalistic misuse of hacker"
  5. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-5) <http://stallman.org/archives/2012-sep-dec.html#06_December_2012_%28Ecuadorian_white_hat_cracker_freed%29>
  6. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-Cybercrime:The_Investigation.2C_Prosecution_and_Defense_of_a_Computer-Related_Crime_6-0) Clifford, Ralph D. (2006). *Cybercrime:The Investigation, Prosecution and Defense of a Computer-Related Crime Second Edition*. Durham, North Carolina: Carolina Academic Press.
  7. ^ [***a***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-hacker_hats_7-0) [***b***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-hacker_hats_7-1) Wilhelm, Douglas (2010). "2". *Professional Penetration Testing*. Syngress Press. p. 503. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-1-59749-425-0](http://en.wikipedia.org/wiki/Special:BookSources/978-1-59749-425-0).
  8. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-8) [EC-Council](http://www.eccouncil.org/)
  9. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-Moore2005_9-0) Moore, Robert (2005). *Cybercrime: Investigating High Technology Computer Crime*. Matthew Bender & Company. p. 258. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [1-59345-303-5](http://en.wikipedia.org/wiki/Special:BookSources/1-59345-303-5).Robert Moore
  10. ^ [***a***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-moore2006_10-0) [***b***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-moore2006_10-1) [***c***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-moore2006_10-2) Moore, Robert (2006). *Cybercrime: Investigating High-Technology Computer Crime* (1st ed.). Cincinnati, Ohio: Anderson Publishing. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-1-59345-303-9](http://en.wikipedia.org/wiki/Special:BookSources/978-1-59345-303-9).
  11. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-thomas2002_11-0) Thomas, Douglas (2002). *Hacker Culture*. University of Minnesota Press. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-8166-3346-3](http://en.wikipedia.org/wiki/Special:BookSources/978-0-8166-3346-3).
  12. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-Andress_10_12-0) Andress, Mandy; Cox, Phil; Tittel, Ed. *CIW Security Professional*. New York, NY: Hungry Minds, Inc.. p. 638. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-7645-4822-0](http://en.wikipedia.org/wiki/Special:BookSources/0-7645-4822-0).
  13. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-13) ["Blue hat hacker Definition"](http://www.pcmag.com/encyclopedia_term/0,2542,t=blue+hat+hacker&i=56321,00.asp). *PC Magazine Encyclopedia*. Retrieved 31 May 2010. "A security professional invited by Microsoft to find vulnerabilities in Windows."
  14. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-14) [Fried, Ina](http://en.wikipedia.org/wiki/Ina_Fried) (June 15, 2005). ["Blue Hat summit meant to reveal ways of the other side"](http://news.cnet.com/Microsoft-meets-the-hackers/2009-1002_3-5747813.html). *Microsoft meets the hackers*. CNET News. Retrieved 31 May 2010.
  15. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-15) [Markoff, John](http://en.wikipedia.org/wiki/John_Markoff) (October 17, 2005). ["At Microsoft, Interlopers Sound Off on Security"](http://www.nytimes.com/2005/10/17/technology/17hackers.html?pagewanted=1&_r=1). *New York Times*. Retrieved 31 May 2010.
  16. ^ [***a***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-GISEC_16-0) [***b***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-GISEC_16-1) [***c***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-GISEC_16-2) Eric Chabrow (February 25, 2012). ["7 Levels of Hackers: Applying An Ancient Chinese Lesson: Know Your Enemies"](http://www.govinfosecurity.com/blogs.php?postID=1206&rf=2012-02-27-eg). GovInfo Security. Retrieved February 27, 2012.
  17. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-17) [Hacking approach](http://www.informit.com/articles/article.aspx?p=25916)
  18. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-bbcprofile_18-0) Writer, Staff (6 September 2012). [Gary McKinnon extradition ruling due by 16 October "Profile: Gary McKinnon"]. BBC News. Retrieved 2012-09-25.
  19. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-19) ["Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution ..."](http://www.usdoj.gov/criminal/cybercrime/mitnick.htm) (Press release). [United States Attorney's Office](http://en.wikipedia.org/wiki/United_States_Attorney%27s_Office), Central District of California. 9 August 1999. Retrieved 10 April 2010.
  20. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-20) Tim Jordan, Paul A. Taylor (2004). *Hacktivism and Cyberwars*. Routledge. pp. 133–134. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-415-26003-9](http://en.wikipedia.org/wiki/Special:BookSources/978-0-415-26003-9). "Wild West imagery has permeated discussions of cybercultures."
  21. ^ [***a***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-thomas_21-0) [***b***](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-thomas_21-1) Thomas, Douglas (2003). *Hacker Culture*. University of Minnesota Press. p. 90. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-8166-3346-3](http://en.wikipedia.org/wiki/Special:BookSources/978-0-8166-3346-3).
  22. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-22) € 19,500
  23. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-23) <http://wetten.overheid.nl/BWBR0001854/TweedeBoek/TitelV/Artikel138ab/geldigheidsdatum_27-12-2012>
  24. [**^**](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29#cite_ref-ntygibson_24-0) Staples, Brent (May 11, 2003). ["A Prince of Cyberpunk Fiction Moves Into the Mainstream"](http://www.nytimes.com/2003/05/11/opinion/11SUN3.html?ex=1367985600&en=9714db46bfff633a&ei=5007&partner=USERLAND). *The New York Times*. Retrieved 2008-08-30. "Mr. Gibson's novels and short stories are worshiped by hackers"[[*dead link*](http://en.wikipedia.org/wiki/Wikipedia:Link_rot)]

**Related literature**

* Kevin Beaver (2010-01-12). [*Hacking For Dummies*](http://books.google.com/?id=ulZ7ln6ORBAC&lpg=PP1&dq=Kevin%20Beaver.%20Hacking%20For%20Dummies.&pg=PP1#v=onepage&q&f=false). [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-7645-5784-2](http://en.wikipedia.org/wiki/Special:BookSources/978-0-7645-5784-2).
* Richard Conway, Julian Cordingley. *Code Hacking: A Developer's Guide to Network Security*. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-1-58450-314-9](http://en.wikipedia.org/wiki/Special:BookSources/978-1-58450-314-9).
* [“Dot.Con: The Dangers of Cyber Crime and a Call for Proactive Solutions,”](http://www.scribd.com/doc/14361572/Dotcon-Dangers-of-Cybercrime-by-Johanna-Granville) by Johanna Granville, *Australian Journal of Politics and History*, vol. 49, no. 1. (Winter 2003), pp. 102–109.
* Katie Hafner & John Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Simon & Schuster. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-671-68322-5](http://en.wikipedia.org/wiki/Special:BookSources/0-671-68322-5).
* David H. Freeman & Charles C. Mann (1997). *@ Large: The Strange Case of the World's Biggest Internet Invasion*. Simon & Schuster. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-684-82464-7](http://en.wikipedia.org/wiki/Special:BookSources/0-684-82464-7).
* Suelette Dreyfus (1997). [*Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*](http://en.wikipedia.org/wiki/Underground_%28Suelette_Dreyfus_book%29). Mandarin. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [1-86330-595-5](http://en.wikipedia.org/wiki/Special:BookSources/1-86330-595-5).
* Bill Apro & Graeme Hammond (2005). *Hackers: The Hunt for Australia's Most Infamous Computer Cracker*. Five Mile Press. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [1-74124-722-5](http://en.wikipedia.org/wiki/Special:BookSources/1-74124-722-5).
* Stuart McClure, Joel Scambray & George Kurtz (1999). *Hacking Exposed*. Mcgraw-Hill. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-07-212127-0](http://en.wikipedia.org/wiki/Special:BookSources/0-07-212127-0).
* Michael Gregg (2006). *Certfied Ethical Hacker*. Pearson. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0-7897-3531-7](http://en.wikipedia.org/wiki/Special:BookSources/978-0-7897-3531-7).
* Clifford Stoll (1990). *The Cuckoo's Egg*. The Bodley Head Ltd. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-370-31433-6](http://en.wikipedia.org/wiki/Special:BookSources/0-370-31433-6).
* Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness & Michael Lester (2004). [*Gray Hat Hacking : The Ethical Hacker's Handbook*](http://books.google.com/?id=jMmpLwe2ezoC&q=gray+hat+hacking&dq=gray+hat+hacking). McGraw-Hill Osborne Media. [ISBN](http://en.wikipedia.org/wiki/International_Standard_Book_Number) [978-0072257090](http://en.wikipedia.org/wiki/Special:BookSources/978-0072257090).

**External links**

|  |  |
| --- | --- |
| http://upload.wikimedia.org/wikipedia/commons/thumb/d/df/Wikibooks-logo-en-noslogan.svg/40px-Wikibooks-logo-en-noslogan.svg.png | Wikibooks has a book on the topic of: [***Hacking***](http://en.wikibooks.org/wiki/Hacking) |

* [CNN Tech PCWorld Staff (November 2001). Timeline: A 40-year history of hacking from 1960 to 2001](http://archives.cnn.com/2001/TECH/internet/11/19/hack.history.idg/)
* [Discovery Channel Documentary. History of Hacking Documentary video](http://vodpod.com/watch/31369-discovery-channel-the-history-of-hacking-documentary)