# Computer security

From Wikipedia, the free encyclopedia

[](https://en.wikipedia.org/wiki/File:Computer_locked.jpg)

While most aspects of computer security involve digital measures such as electronic passwords and encryption, physical security measures such as metal locks are still used to prevent unauthorized tampering.

**Computer security**, **cybersecurity**[[1]](https://en.wikipedia.org/wiki/Computer_security#cite_note-1) or **information technology security** (**IT security**) is the protection of [computer systems](https://en.wikipedia.org/wiki/Computer_system) and [networks](https://en.wikipedia.org/wiki/Computer_network) from the theft of or damage to their [hardware](https://en.wikipedia.org/wiki/Computer_hardware), [software](https://en.wikipedia.org/wiki/Software), or [electronic data](https://en.wikipedia.org/wiki/Data_(computing)), as well as from the [disruption](https://en.wikipedia.org/wiki/Denial-of-service_attack) or [misdirection](https://en.wikipedia.org/wiki/Botnet) of the services they provide.

The field is becoming more important due to increased reliance on [computer systems](https://en.wikipedia.org/wiki/Computer_systems), the [Internet](https://en.wikipedia.org/wiki/Internet)[[2]](https://en.wikipedia.org/wiki/Computer_security#cite_note-2) and [wireless network](https://en.wikipedia.org/wiki/Wireless_network) standards such as [Bluetooth](https://en.wikipedia.org/wiki/Bluetooth) and [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi), and due to the growth of ["smart" devices](https://en.wikipedia.org/wiki/Smart_devices), including [smartphones](https://en.wikipedia.org/wiki/Smartphone), [televisions](https://en.wikipedia.org/wiki/Television), and the various devices that constitute the "[Internet of things](https://en.wikipedia.org/wiki/Internet_of_things)". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world.[[3]](https://en.wikipedia.org/wiki/Computer_security#cite_note-3)

## Vulnerabilities and attacks[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=1)]

*Main article:*[*Vulnerability (computing)*](https://en.wikipedia.org/wiki/Vulnerability_(computing))

A vulnerability is a weakness in design, implementation, operation, or internal control. Most of the vulnerabilities that have been discovered are documented in the [Common Vulnerabilities and Exposures](https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures) (CVE) database. An *exploitable* vulnerability is one for which at least one working attack or "[exploit"](https://en.wikipedia.org/wiki/Exploit_(computer_security)) exists.[[4]](https://en.wikipedia.org/wiki/Computer_security#cite_note-4) Vulnerabilities can be researched, reverse-engineered, hunted, or exploited using [automated tools](https://en.wikipedia.org/wiki/Automated_threat) or customized scripts.[[5]](https://en.wikipedia.org/wiki/Computer_security#cite_note-5)[[6]](https://en.wikipedia.org/wiki/Computer_security#cite_note-6) To secure a computer system, it is important to understand the attacks that can be made against it, and these [threats](https://en.wikipedia.org/wiki/Threat_(computer)) can typically be classified into one of these categories below:

### Backdoor**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=2)**]**

A [backdoor](https://en.wikipedia.org/wiki/Backdoor_(computing)) in a computer system, a [cryptosystem](https://en.wikipedia.org/wiki/Cryptosystem) or an [algorithm](https://en.wikipedia.org/wiki/Algorithm), is any secret method of bypassing normal [authentication](https://en.wikipedia.org/wiki/Authentication) or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may have been added by an authorised party to allow some legitimate access, or by an attacker for malicious reasons; but regardless of the motives for their existence, they create a vulnerability. Backdoors can be very hard to detect, and detection of backdoors are usually discovered by someone who has access to application source code or intimate knowledge of the computer's Operating System.

### Denial-of-service attack**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=3)**]**

[Denial of service attacks](https://en.wikipedia.org/wiki/Denial_of_service_attacks) (DoS) are designed to make a machine or network resource unavailable to its intended users.[[7]](https://en.wikipedia.org/wiki/Computer_security#cite_note-7) Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim's account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single [IP address](https://en.wikipedia.org/wiki/IP_address) can be blocked by adding a new firewall rule, many forms of [Distributed denial of service](https://en.wikipedia.org/wiki/Distributed_denial_of_service#Distributed_attack) (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult. Such attacks can originate from the [zombie computers](https://en.wikipedia.org/wiki/Zombie_computer) of a [botnet](https://en.wikipedia.org/wiki/Botnet) or from a range of other possible techniques, including [reflection and amplification attacks](https://en.wikipedia.org/wiki/Distributed_Reflection_Denial_of_Service), where innocent systems are fooled into sending traffic to the victim.

### Direct-access attacks**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=4)**]**

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. They may also compromise security by making [operating system](https://en.wikipedia.org/wiki/Operating_system) modifications, installing software [worms](https://en.wikipedia.org/wiki/Computer_worm), [keyloggers](https://en.wikipedia.org/wiki/Keystroke_logging), [covert listening devices](https://en.wikipedia.org/wiki/Covert_listening_device) or using wireless mice. Even when the system is protected by standard security measures, these may be able to be by-passed by booting another operating system or tool from a [CD-ROM](https://en.wikipedia.org/wiki/CD-ROM) or other bootable media. [Disk encryption](https://en.wikipedia.org/wiki/Disk_encryption) and [Trusted Platform Module](https://en.wikipedia.org/wiki/Trusted_Platform_Module) are designed to prevent these attacks.

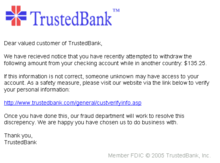
### Eavesdropping**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=5)**]**

[Eavesdropping](https://en.wikipedia.org/wiki/Eavesdropping) is the act of surreptitiously listening to a private computer "conversation" (communication), typically between hosts on a network. For instance, programs such as [Carnivore](https://en.wikipedia.org/wiki/Carnivore_(FBI)) and [NarusInSight](https://en.wikipedia.org/wiki/Narus_(company)) have been used by the [FBI](https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation) and [NSA](https://en.wikipedia.org/wiki/National_Security_Agency) to eavesdrop on the systems of [internet service providers](https://en.wikipedia.org/wiki/Internet_service_provider). Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint [electromagnetic](https://en.wikipedia.org/wiki/Electromagnetism) transmissions generated by the hardware; [TEMPEST](https://en.wikipedia.org/wiki/TEMPEST) is a specification by the [NSA](https://en.wikipedia.org/wiki/National_Security_Agency) referring to these attacks.

### Multi-vector, polymorphic attacks**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=6)**]**

Surfacing in 2017, a new class of multi-vector,[[8]](https://en.wikipedia.org/wiki/Computer_security#cite_note-8) polymorphic[[9]](https://en.wikipedia.org/wiki/Computer_security#cite_note-9) cyber threats surfaced that combined several types of attacks and changed form to avoid cybersecurity controls as they spread. These threats have been classified as fifth-generation cyberattacks.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

### Phishing**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=7)**]**

[](https://en.wikipedia.org/wiki/File:PhishingTrustedBank.png)

An example of a phishing email, disguised as an official [email](https://en.wikipedia.org/wiki/Email) from a (fictional) bank. The sender is attempting to trick the recipient into revealing confidential information by "confirming" it at the phisher's website. Note the misspelling of the words *received* and *discrepancy* as *received* and *discrepancy*, respectively. Although the [URL](https://en.wikipedia.org/wiki/URL) of the bank's [webpage](https://en.wikipedia.org/wiki/Webpage) appears to be legitimate, the hyperlink points at the phisher's webpage.

[Phishing](https://en.wikipedia.org/wiki/Phishing) is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users by deceiving the users.[[10]](https://en.wikipedia.org/wiki/Computer_security#cite_note-10) Phishing is typically carried out by [email spoofing](https://en.wikipedia.org/wiki/Email_spoofing) or [instant messaging](https://en.wikipedia.org/wiki/Instant_messaging), and it often directs users to enter details at a fake website whose "look" and "feel" are almost identical to the legitimate one. The fake website often asks for personal information, such as log-in details and passwords. This information can then be used to gain access to the individual's real account on the real website. Preying on a victim's trust, phishing can be classified as a form of [social engineering](https://en.wikipedia.org/wiki/Social_engineering_(computer_security)). Attackers are using creative ways to gain access to real accounts. A common scam is for attackers to send fake electronic invoices[[11]](https://en.wikipedia.org/wiki/Computer_security#cite_note-11) to individuals showing that they recently purchased music, apps, or other, and instructing them to click on a link if the purchases were not authorized.

### Privilege escalation**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=8)**]**

[Privilege escalation](https://en.wikipedia.org/wiki/Privilege_escalation) describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to [exploit](https://en.wikipedia.org/wiki/Exploit_(computer_security)) a [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) in the system to gain access to restricted data; or even become "[root](https://en.wikipedia.org/wiki/Superuser)" and have full unrestricted access to a system.

### Reverse engineering**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=9)**]**

[Reverse engineering](https://en.wikipedia.org/wiki/Reverse_engineering) is the process by which a man-made object is deconstructed to reveal its designs, code, architecture, or to extract knowledge from the object; similar to scientific research, the only difference being that scientific research is about a natural phenomenon.[[12]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Eilam-12):3

### Social engineering**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=10)**]**

[Social engineering](https://en.wikipedia.org/wiki/Social_engineering_(computer_security)), insofar as computer security is concerned, aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer.[[13]](https://en.wikipedia.org/wiki/Computer_security#cite_note-13)

Social engineering, in the context of information security, is the psychological manipulation of people into performing actions or divulging confidential information.

A common scam involves fake CEO emails sent to accounting and finance departments. In early 2016, the [FBI](https://en.wikipedia.org/wiki/FBI) reported that the scam has cost US businesses more than $2 billion in about two years.[[14]](https://en.wikipedia.org/wiki/Computer_security#cite_note-14)

In May 2016, the [Milwaukee Bucks](https://en.wikipedia.org/wiki/Milwaukee_Bucks) [NBA](https://en.wikipedia.org/wiki/NBA) team was the victim of this type of cyber scam with a perpetrator impersonating the team's president [Peter Feigin](https://en.wikipedia.org/w/index.php?title=Peter_Feigin&action=edit&redlink=1), resulting in the handover of all the team's employees' 2015 [W-2](https://en.wikipedia.org/wiki/Form_W-2) tax forms.[[15]](https://en.wikipedia.org/wiki/Computer_security#cite_note-15)

### Spoofing**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=11)**]**

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

Spoofing is the act of masquerading as a valid entity through falsification of data (such as an [IP address](https://en.wikipedia.org/wiki/IP_address) or username), in order to gain access to information or resources that one is otherwise unauthorized to obtain.[[16]](https://en.wikipedia.org/wiki/Computer_security#cite_note-techopedia-16)[[17]](https://en.wikipedia.org/wiki/Computer_security#cite_note-17) There are several types of spoofing, including:

* [Email spoofing](https://en.wikipedia.org/wiki/Email_spoofing), where an attacker forges the sending (*From*, or source) address of an email.
* [IP address spoofing](https://en.wikipedia.org/wiki/IP_address_spoofing), where an attacker alters the source IP address in a [network packet](https://en.wikipedia.org/wiki/Network_packet) to hide their identity or impersonate another computing system.
* [MAC spoofing](https://en.wikipedia.org/wiki/MAC_spoofing), where an attacker modifies the [Media Access Control (MAC) address](https://en.wikipedia.org/wiki/MAC_address) of their [network interface](https://en.wikipedia.org/wiki/Network_interface) to pose as a valid user on a network.
* [Biometric](https://en.wikipedia.org/wiki/Biometrics) spoofing, where an attacker produces a fake biometric sample to pose as another user.[[18]](https://en.wikipedia.org/wiki/Computer_security#cite_note-18)

### Tampering**[**[**edit**](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=12)**]**

[Tampering](https://en.wikipedia.org/wiki/Tampering_(crime)) describes a malicious modification or alteration of data. So-called [Evil Maid attacks](https://en.wikipedia.org/wiki/Evil_Maid_attack) and security services planting of [surveillance](https://en.wikipedia.org/wiki/Surveillance) capability into routers are examples.[[19]](https://en.wikipedia.org/wiki/Computer_security#cite_note-19)

## Information security culture[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=13)]

Employee behavior can have a big impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within an organization. Information security culture is the "...totality of patterns of behavior in an organization that contributes to the protection of information of all kinds.″[[20]](https://en.wikipedia.org/wiki/Computer_security#cite_note-20)

Andersson and Reimers (2014) found that employees often do not see themselves as part of their organization's information security effort and often take actions that impede organizational changes.[[21]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Reimers2017-21) Research shows information security culture needs to be improved continuously. In ″Information Security Culture from Analysis to Change″, authors commented, ″It's a never-ending process, a cycle of evaluation and change or maintenance.″ To manage the information security culture, five steps should be taken: pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.[[22]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Schlienger,_Thomas_2003-22)

* Pre-Evaluation: to identify the awareness of information security within employees and to analyze the current security policy.
* Strategic Planning: to come up with a better awareness program, clear targets need to be set. Assembling a team of skilled professionals is helpful to achieve it.
* Operative Planning: a good security culture can be established based on internal communication, management-buy-in, and security awareness and a training program.[[22]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Schlienger,_Thomas_2003-22)
* Implementation: four stages should be used to implement the information security culture. They are:

1. Commitment of the management
2. Communication with organizational members
3. Courses for all organizational members
4. Commitment of the employees[[22]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Schlienger,_Thomas_2003-22)

* Post-Evaluation: to assess the success of the planning and implementation, and to identify unresolved areas of concern.