# Definition of cyber security

**Computer security**, also known as **cyber security** or **IT security**, is the protection of [information systems](https://en.wikipedia.org/wiki/Information_system) from theft or damage to the [hardware](https://en.wikipedia.org/wiki/Computer_hardware), the [software](https://en.wikipedia.org/wiki/Software), and to the [information](https://en.wikipedia.org/wiki/Information) on them, as well as from [disruption](https://en.wikipedia.org/wiki/Denial-of-service_attack) or [misdirection](https://en.wikipedia.org/wiki/Botnet) of the services they provide.

It includes [controlling physical access](https://en.wikipedia.org/wiki/Physical_security) to the hardware, as well as protecting against harm that may come via [network access](https://en.wikipedia.org/wiki/Computer_network), [data](https://en.wikipedia.org/wiki/SQL_injection) and [code injection](https://en.wikipedia.org/wiki/Code_injection), and due to malpractice by operators, whether [intentional](https://en.wikipedia.org/wiki/Insider_threat), [accidental](https://en.wikipedia.org/wiki/Error-tolerant_design), or due to them [being tricked](https://en.wikipedia.org/wiki/Social_engineering_(security)) into deviating from secure procedures.

The field is of growing importance due to the increasing reliance on computer systems in most societies and the growth of ["smart" devices](https://en.wikipedia.org/wiki/Smart_devices), including [smartphones](https://en.wikipedia.org/wiki/Smartphones), [televisions](https://en.wikipedia.org/wiki/Television) and tiny devices as part of the [Internet of Things](https://en.wikipedia.org/wiki/Internet_of_Things) – and of the [Internet](https://en.wikipedia.org/wiki/Internet) and [wireless network](https://en.wikipedia.org/wiki/Wireless_network) such as [Bluetooth](https://en.wikipedia.org/wiki/Bluetooth) and [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi).

There are related security categories, which are: [Internet security](https://en.wikipedia.org/wiki/Internet_security), [Cyber warfare](https://en.wikipedia.org/wiki/Cyberwarfare), [Information security](https://en.wikipedia.org/wiki/Information_security), [Mobile security](https://en.wikipedia.org/wiki/Mobile_security) and [Network security](https://en.wikipedia.org/wiki/Network_security).

# Vulnerabilities and attacks

There are a different number of vulnerabilities and attacks, these are documented in CVE (Common Vulnerabilities and Exposures) database, and the vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities as they are discovered.

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 be classified into one of the categories below:

* **Backdoors** = A backdoor is when there is an unauthorized access to a computer program that bypasses security mechanisms.
* **Denial-of-service (DoS) attack** = this is a type of attack where the hacker is targeting the shutting or the damage of the network by flooding it with useless traffic.
* **Direct – access attack** = This is when unauthorized user gaining physical access to a computer is most likely able to direct 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), [key loggers](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.
* **Eavesdropping** = Eavesdropping is the act of surreptitiously listening to a private conversation, 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 [electro-magnetic](https://en.wikipedia.org/wiki/Electromagnetism) transmissions generated by the hardware
* **Spoofing** = Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spoofing is most prevalent in communication mechanisms that lack a [high level of security.](https://www.techopedia.com/definition/5398/spoofing)
* **Tampering** = [Tampering](https://en.wikipedia.org/wiki/Tampering_(crime)) describes a malicious modification of products. So-called ["Evil Maid" attacks](https://en.wikipedia.org/wiki/Rootkit#bootkit) and security services planting of surveillance capability into routers[[6]](https://en.wikipedia.org/wiki/Computer_security#cite_note-6) are examples.
* **Privilege escalation** = [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. So for example, a standard computer user may be able to fool the system into giving them access to restricted data; or even to "[become root](https://en.wikipedia.org/wiki/Superuser)" and have full-unrestricted access to a system.
* **Phishing** = [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. Phishing is typically carried out by email spoofing or 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. Preying on a victim's trusting, phishing can be classified as a form of [social engineering](https://en.wikipedia.org/wiki/Social_engineering_(computer_security)).
* **Clickjacking** = It is known also as UI redress attack or User Interface redress attack, and this is done by the attacker tricking the user in believing that he is entering the right details into the right place, but the attacker has probably creating a series of buttons and links, which can be made by multiple transparent or opaque layers. This is “HIJACKING” the clicks and routing them into some irrelevant page, most likely to be owned by someone else.
* **Social engineering** = It aims to convince a user to disclose secrets such as passwords, card numbers. For example, they could be impersonating a bank, a contractor, or a customer.
* **Cryptographic attacks** = This is a method for circumventing the security of a **cryptographic** system by finding a weakness in a code, cipher, **cryptographic** protocol or key management scheme.
  + Attacks on public – key cryptosystems
  + Chosen – plaintext attacks
  + Cryptanalytic software
  + Password cracking software
  + Ransomware
  + Side – channel attacks

Bibliography

<http://computersecurity.wikia.com/wiki/Backdoor>