Computer security

From Wikipedia, the free encyclopedia

|  |
| --- |
| This article is part of a series on |
| **Computer security** |
| * **Computer security** (main article) |
| **Related security categories** |
| * [Internet security](https://en.wikipedia.org/wiki/Internet_security) * [Cyberwarfare](https://en.wikipedia.org/wiki/Cyberwarfare) * [Information security](https://en.wikipedia.org/wiki/Information_security) * [Mobile security](https://en.wikipedia.org/wiki/Mobile_security) * [Network security](https://en.wikipedia.org/wiki/Network_security) |
| **Threats** |
| * [Computer crime](https://en.wikipedia.org/wiki/Computer_crime) * [Vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) * [Eavesdropping](https://en.wikipedia.org/wiki/Eavesdropping) * [Exploits](https://en.wikipedia.org/wiki/Exploit_(computer_security)) * [Trojans](https://en.wikipedia.org/wiki/Trojan_horse_(computing)) * [Viruses](https://en.wikipedia.org/wiki/Computer_virus) and [worms](https://en.wikipedia.org/wiki/Computer_worm) * [Denial of service](https://en.wikipedia.org/wiki/Denial_of_service) * [Malware](https://en.wikipedia.org/wiki/Malware) * [Payloads](https://en.wikipedia.org/wiki/Payload_(computing)) * [Rootkits](https://en.wikipedia.org/wiki/Rootkit) * [Keyloggers](https://en.wikipedia.org/wiki/Keylogger) |
| **Defenses** |
| * [Access Control Systems](https://en.wikipedia.org/wiki/Access_Control_Systems) * [Application security](https://en.wikipedia.org/wiki/Application_security)   + [Antivirus software](https://en.wikipedia.org/wiki/Antivirus_software)   + [Secure coding](https://en.wikipedia.org/wiki/Secure_coding)   + [Security by design](https://en.wikipedia.org/wiki/Security_by_design)   + [Secure operating systems](https://en.wikipedia.org/wiki/Security-focused_operating_system) * [Authentication](https://en.wikipedia.org/wiki/Authentication)   + [Multi-factor authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication)   + [Two-factor authentication](https://en.wikipedia.org/wiki/Two-factor_authentication) * [Authorization](https://en.wikipedia.org/wiki/Authorization) * [Data-centric security](https://en.wikipedia.org/wiki/Data-centric_security) * [Firewall (computing)](https://en.wikipedia.org/wiki/Firewall_(computing)) * [Intrusion detection system](https://en.wikipedia.org/wiki/Intrusion_detection_system) * [Intrusion prevention system](https://en.wikipedia.org/wiki/Intrusion_prevention_system) * [Mobile secure gateway](https://en.wikipedia.org/wiki/Mobile_secure_gateway) |
| * [v](https://en.wikipedia.org/wiki/Template:Computer_security) * [t](https://en.wikipedia.org/wiki/Template_talk:Computer_security) * [e](https://en.wikipedia.org/w/index.php?title=Template:Computer_security&action=edit) |

**Computer security**, also known as **cyber security** or [**IT**](https://en.wikipedia.org/wiki/Information_technology)**security**, is the protection of [computer systems](https://en.wikipedia.org/wiki/Computer_system) from the theft or damage to the [hardware](https://en.wikipedia.org/wiki/Computer_hardware), [software](https://en.wikipedia.org/wiki/Software) or 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.[[1]](https://en.wikipedia.org/wiki/Computer_security#cite_note-1)

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),[[2]](https://en.wikipedia.org/wiki/Computer_security#cite_note-2) 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.[[3]](https://en.wikipedia.org/wiki/Computer_security#cite_note-3)

The field is of growing importance due to the increasing reliance on computer systems and the [Internet](https://en.wikipedia.org/wiki/Internet) in most societies,[[4]](https://en.wikipedia.org/wiki/Computer_security#cite_note-4) [wireless networks](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) – and 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 tiny devices as part of the [Internet of Things](https://en.wikipedia.org/wiki/Internet_of_Things).

**Contents**

  [hide]

* [1Vulnerabilities and attacks](https://en.wikipedia.org/wiki/Computer_security#Vulnerabilities_and_attacks)
  + [1.1Backdoors](https://en.wikipedia.org/wiki/Computer_security#Backdoors)
  + [1.2Denial-of-service attack](https://en.wikipedia.org/wiki/Computer_security#Denial-of-service_attack)
  + [1.3Direct-access attacks](https://en.wikipedia.org/wiki/Computer_security#Direct-access_attacks)
  + [1.4Eavesdropping](https://en.wikipedia.org/wiki/Computer_security#Eavesdropping)
  + [1.5Spoofing](https://en.wikipedia.org/wiki/Computer_security#Spoofing)
  + [1.6Tampering](https://en.wikipedia.org/wiki/Computer_security#Tampering)
  + [1.7Privilege escalation](https://en.wikipedia.org/wiki/Computer_security#Privilege_escalation)
  + [1.8Phishing](https://en.wikipedia.org/wiki/Computer_security#Phishing)
  + [1.9Clickjacking](https://en.wikipedia.org/wiki/Computer_security#Clickjacking)
  + [1.10Social engineering](https://en.wikipedia.org/wiki/Computer_security#Social_engineering)
* [2Systems at risk](https://en.wikipedia.org/wiki/Computer_security#Systems_at_risk)
  + [2.1Financial systems](https://en.wikipedia.org/wiki/Computer_security#Financial_systems)
  + [2.2Utilities and industrial equipment](https://en.wikipedia.org/wiki/Computer_security#Utilities_and_industrial_equipment)
  + [2.3Aviation](https://en.wikipedia.org/wiki/Computer_security#Aviation)
  + [2.4Consumer devices](https://en.wikipedia.org/wiki/Computer_security#Consumer_devices)
  + [2.5Large corporations](https://en.wikipedia.org/wiki/Computer_security#Large_corporations)
  + [2.6Automobiles](https://en.wikipedia.org/wiki/Computer_security#Automobiles)
  + [2.7Government](https://en.wikipedia.org/wiki/Computer_security#Government)
  + [2.8Internet of Things and physical vulnerabilities](https://en.wikipedia.org/wiki/Computer_security#Internet_of_Things_and_physical_vulnerabilities)
* [3Impact of security breaches](https://en.wikipedia.org/wiki/Computer_security#Impact_of_security_breaches)
* [4Attacker motivation](https://en.wikipedia.org/wiki/Computer_security#Attacker_motivation)
* [5Computer protection (countermeasures)](https://en.wikipedia.org/wiki/Computer_security#Computer_protection_.28countermeasures.29)
  + [5.1Security by design](https://en.wikipedia.org/wiki/Computer_security#Security_by_design)
  + [5.2Security architecture](https://en.wikipedia.org/wiki/Computer_security#Security_architecture)
  + [5.3Security measures](https://en.wikipedia.org/wiki/Computer_security#Security_measures)
  + [5.4Vulnerability management](https://en.wikipedia.org/wiki/Computer_security#Vulnerability_management)
  + [5.5Reducing vulnerabilities](https://en.wikipedia.org/wiki/Computer_security#Reducing_vulnerabilities)
  + [5.6Hardware protection mechanisms](https://en.wikipedia.org/wiki/Computer_security#Hardware_protection_mechanisms)
  + [5.7Secure operating systems](https://en.wikipedia.org/wiki/Computer_security#Secure_operating_systems)
  + [5.8Secure coding](https://en.wikipedia.org/wiki/Computer_security#Secure_coding)
  + [5.9Capabilities and access control lists](https://en.wikipedia.org/wiki/Computer_security#Capabilities_and_access_control_lists)
  + [5.10Response to breaches](https://en.wikipedia.org/wiki/Computer_security#Response_to_breaches)
* [6Notable attacks and breaches](https://en.wikipedia.org/wiki/Computer_security#Notable_attacks_and_breaches)
  + [6.1Robert Morris and the first computer worm](https://en.wikipedia.org/wiki/Computer_security#Robert_Morris_and_the_first_computer_worm)
  + [6.2Rome Laboratory](https://en.wikipedia.org/wiki/Computer_security#Rome_Laboratory)
  + [6.3TJX customer credit card details](https://en.wikipedia.org/wiki/Computer_security#TJX_customer_credit_card_details)
  + [6.4Stuxnet attack](https://en.wikipedia.org/wiki/Computer_security#Stuxnet_attack)
  + [6.5Global surveillance disclosures](https://en.wikipedia.org/wiki/Computer_security#Global_surveillance_disclosures)
  + [6.6Target and Home Depot breaches](https://en.wikipedia.org/wiki/Computer_security#Target_and_Home_Depot_breaches)
  + [6.7Ashley Madison breach](https://en.wikipedia.org/wiki/Computer_security#Ashley_Madison_breach)
* [7Legal issues and global regulation](https://en.wikipedia.org/wiki/Computer_security#Legal_issues_and_global_regulation)
* [8Government](https://en.wikipedia.org/wiki/Computer_security#Government_2)
* [9Actions and teams in the US](https://en.wikipedia.org/wiki/Computer_security#Actions_and_teams_in_the_US)
  + [9.1Legislation](https://en.wikipedia.org/wiki/Computer_security#Legislation)
  + [9.2Agencies](https://en.wikipedia.org/wiki/Computer_security#Agencies)
  + [9.3Computer emergency readiness team](https://en.wikipedia.org/wiki/Computer_security#Computer_emergency_readiness_team)
* [10International actions](https://en.wikipedia.org/wiki/Computer_security#International_actions)
  + [10.1Europe](https://en.wikipedia.org/wiki/Computer_security#Europe)
* [11National teams](https://en.wikipedia.org/wiki/Computer_security#National_teams)
  + [11.1Canada](https://en.wikipedia.org/wiki/Computer_security#Canada)
  + [11.2China](https://en.wikipedia.org/wiki/Computer_security#China)
  + [11.3Germany](https://en.wikipedia.org/wiki/Computer_security#Germany)
  + [11.4India](https://en.wikipedia.org/wiki/Computer_security#India)
  + [11.5Pakistan](https://en.wikipedia.org/wiki/Computer_security#Pakistan)
  + [11.6South Korea](https://en.wikipedia.org/wiki/Computer_security#South_Korea)
  + [11.7Other countries](https://en.wikipedia.org/wiki/Computer_security#Other_countries)
* [12Modern warfare](https://en.wikipedia.org/wiki/Computer_security#Modern_warfare)
* [13Job market](https://en.wikipedia.org/wiki/Computer_security#Job_market)
* [14Terminology](https://en.wikipedia.org/wiki/Computer_security#Terminology)
* [15Scholars](https://en.wikipedia.org/wiki/Computer_security#Scholars)
* [16See also](https://en.wikipedia.org/wiki/Computer_security#See_also)
* [17Further reading](https://en.wikipedia.org/wiki/Computer_security#Further_reading)
* [18References](https://en.wikipedia.org/wiki/Computer_security#References)
* [19External links](https://en.wikipedia.org/wiki/Computer_security#External_links)

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 system susceptibility or flaw. Many vulnerabilities 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.[[5]](https://en.wikipedia.org/wiki/Computer_security#cite_note-5)

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 the categories below:

**Backdoors**[[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, is any secret method of bypassing normal 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 authorized 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.

**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) (DDoS) are designed to make a machine or network resource unavailable to its intended users.[[6]](https://en.wikipedia.org/wiki/Computer_security#cite_note-6) Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim 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 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) 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), but a range of other techniques are possible including [reflection and amplification attacks](https://en.wikipedia.org/wiki/Denial-of-service_attack#Reflected_.2F_spoofed_attack), 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.[[7]](https://en.wikipedia.org/wiki/Computer_security#cite_note-7) 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 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; [TEMPEST](https://en.wikipedia.org/wiki/TEMPEST) is a specification by the NSA referring to these attacks.

**Spoofing**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=6)]

[Spoofing](https://en.wikipedia.org/wiki/Spoofing_attack), 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.[[8]](https://en.wikipedia.org/wiki/Computer_security#cite_note-8)

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

[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[[9]](https://en.wikipedia.org/wiki/Computer_security#cite_note-9) are examples.

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

[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.[[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. 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)).

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

[Clickjacking](https://en.wikipedia.org/wiki/Clickjacking), also known as "UI redress attack" or "User Interface redress attack", is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically "[hijacking](https://en.wikipedia.org/wiki/Page_hijacking)" the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of stylesheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

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

*Main article:*[*Social engineering (security)*](https://en.wikipedia.org/wiki/Social_engineering_(security))

*See also:*[*Category:Cryptographic attacks*](https://en.wikipedia.org/wiki/Category:Cryptographic_attacks)

[Social engineering](https://en.wikipedia.org/wiki/Social_engineering_(computer_security)) 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.[[11]](https://en.wikipedia.org/wiki/Computer_security#cite_note-11)

A popular and profitable cyber 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 $2bn in about two years.[[12]](https://en.wikipedia.org/wiki/Computer_security#cite_note-12)

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.[[13]](https://en.wikipedia.org/wiki/Computer_security#cite_note-13)

Systems at risk[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=12)]

Computer security is critical in almost any industry which uses computers. Currently, most electronic devices such as computers, laptops and cellphones come with built in firewall security software, but despite this, computers are not 100 percent accurate and dependable to protect our data (Smith, Grabosky & Urbas, 2004.) There are many different ways of hacking into computers. It can be done through a network system, clicking into unknown links, connecting to unfamiliar Wi-Fi, downloading software and files from unsafe sites, power consumption, electromagnetic radiation waves, and many more. However, computers can be protected through well built software and hardware. By having strong internal interactions of properties, software complexity can prevent software crash and security failure.[[14]](https://en.wikipedia.org/wiki/Computer_security#cite_note-FAA_Computer_Security-14)

**Financial systems**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=13)]

Web sites and apps that accept or store [credit card numbers](https://en.wikipedia.org/wiki/Credit_card_number), brokerage accounts, and [bank account](https://en.wikipedia.org/wiki/Bank_account) information are prominent hacking targets, because of the potential for immediate financial gain from transferring money, making purchases, or selling the information on the [black market](https://en.wikipedia.org/wiki/Black_market).[[15]](https://en.wikipedia.org/wiki/Computer_security#cite_note-15) In-store payment systems and [ATMs](https://en.wikipedia.org/wiki/Automated_teller_machine) have also been tampered with in order to gather customer account data and [PINs](https://en.wikipedia.org/wiki/Personal_identification_number).

**Utilities and industrial equipment**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=14)]

Computers control functions at many utilities, including coordination of [telecommunications](https://en.wikipedia.org/wiki/Telecommunications), the [power grid](https://en.wikipedia.org/wiki/Power_grid), [nuclear power plants](https://en.wikipedia.org/wiki/Nuclear_power_plant), and valve opening and closing in water and gas networks. The Internet is a potential attack vector for such machines if connected, but the [Stuxnet](https://en.wikipedia.org/wiki/Stuxnet) worm demonstrated that even equipment controlled by computers not connected to the Internet can be vulnerable to physical damage caused by malicious commands sent to industrial equipment (in that case [uranium enrichment](https://en.wikipedia.org/wiki/Uranium_enrichment) centrifuges) which are infected via [removable media](https://en.wikipedia.org/wiki/Removable_media). In 2014, the [Computer Emergency Readiness Team](https://en.wikipedia.org/wiki/Computer_Emergency_Readiness_Team), a division of the [Department of Homeland Security](https://en.wikipedia.org/wiki/Department_of_Homeland_Security), investigated 79 hacking incidents at energy companies.[[16]](https://en.wikipedia.org/wiki/Computer_security#cite_note-16) Vulnerabilities in [smart meters](https://en.wikipedia.org/wiki/Smart_meter) (many of which use local radio or cellular communications) can cause problems with billing fraud.[[17]](https://en.wikipedia.org/wiki/Computer_security#cite_note-17)

**Aviation**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=15)]

The [aviation](https://en.wikipedia.org/wiki/Aviation) industry is very reliant on a series of complex system which could be attacked.[[18]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Computer_Security_in_Aviation-18) A simple power outage at one airport can cause repercussions worldwide,[[19]](https://en.wikipedia.org/wiki/Computer_security#cite_note-19) much of the system relies on radio transmissions which could be disrupted,[[20]](https://en.wikipedia.org/wiki/Computer_security#cite_note-20) and controlling aircraft over oceans is especially dangerous because radar surveillance only extends 175 to 225 miles offshore.[[21]](https://en.wikipedia.org/wiki/Computer_security#cite_note-21) There is also potential for attack from within an aircraft.[[22]](https://en.wikipedia.org/wiki/Computer_security#cite_note-22)

In Europe, with the ([Pan-European Network Service](https://en.wikipedia.org/wiki/Pan-European_Network_Service))[[23]](https://en.wikipedia.org/wiki/Computer_security#cite_note-23) and NewPENS,[[24]](https://en.wikipedia.org/wiki/Computer_security#cite_note-24) and in the US with the NextGen program,[[25]](https://en.wikipedia.org/wiki/Computer_security#cite_note-25) [air navigation service providers](https://en.wikipedia.org/wiki/Air_navigation_service_provider) are moving to create their own dedicated networks.

The consequences of a successful attack range from loss of confidentiality to loss of system integrity, which may lead to more serious concerns such as exfiltration of data, network and [air traffic control](https://en.wikipedia.org/wiki/Air_traffic_control) outages, which in turn can lead to airport closures, loss of aircraft, loss of passenger life, [damages on the ground](https://en.wikipedia.org/wiki/Collapse_of_the_World_Trade_Center) and to transportation infrastructure. A successful attack on a [military aviation](https://en.wikipedia.org/wiki/Military_aviation) system that controls [munitions](https://en.wikipedia.org/wiki/Munitions) could have even more serious consequences.

**Consumer devices**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=16)]

Desktop computers and laptops are commonly infected with malware either to gather passwords or financial account information, or to construct a [botnet](https://en.wikipedia.org/wiki/Botnet) to attack another target. [Smart phones](https://en.wikipedia.org/wiki/Samsung_Galaxy_Note_3), [tablet computers](https://en.wikipedia.org/wiki/Tablet_computer), [smart watches](https://en.wikipedia.org/wiki/Smart_watch), and other [mobile devices](https://en.wikipedia.org/wiki/Mobile_devices) such as [Quantified Self](https://en.wikipedia.org/wiki/Quantified_Self) devices like [activity trackers](https://en.wikipedia.org/wiki/Activity_tracker) have also become targets and many of these have sensors such as cameras, microphones, GPS receivers, compasses, and [accelerometers](https://en.wikipedia.org/wiki/Accelerometers) which could be exploited, and may collect personal information, including sensitive health information. Wifi, Bluetooth, and cell phone networks on any of these devices could be used as attack vectors, and sensors might be remotely activated after a successful breach.[[26]](https://en.wikipedia.org/wiki/Computer_security#cite_note-nestwatch-26)

[Home automation](https://en.wikipedia.org/wiki/Home_automation) devices such as the [Nest thermostat](https://en.wikipedia.org/wiki/Nest_thermostat) are also potential targets.[[26]](https://en.wikipedia.org/wiki/Computer_security#cite_note-nestwatch-26)

**Large corporations**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=17)]

Large corporations are common targets. In many cases this is aimed at financial gain through identity theft and involves [data breaches](https://en.wikipedia.org/wiki/Data_breach) such as the loss of millions of clients' credit card details by [Home Depot](https://en.wikipedia.org/wiki/Home_Depot),[[27]](https://en.wikipedia.org/wiki/Computer_security#cite_note-27) [Staples](https://en.wikipedia.org/wiki/Staples_Inc.),[[28]](https://en.wikipedia.org/wiki/Computer_security#cite_note-28) and [Target Corporation](https://en.wikipedia.org/wiki/Target_Corporation).[[29]](https://en.wikipedia.org/wiki/Computer_security#cite_note-milwaukee-29) Medical records have been targeted for use in general identify theft, health insurance fraud, and impersonating patients to obtain prescription drugs for recreational purposes or resale.[[30]](https://en.wikipedia.org/wiki/Computer_security#cite_note-30)

Not all attacks are financially motivated however; for example security firm [HBGary Federal](https://en.wikipedia.org/wiki/HBGary_Federal) suffered a serious series of attacks in 2011 from hacktivist group [Anonymous](https://en.wikipedia.org/wiki/Anonymous_(group)) in retaliation for the firm's CEO claiming to have infiltrated their group, [[31]](https://en.wikipedia.org/wiki/Computer_security#cite_note-31)[[32]](https://en.wikipedia.org/wiki/Computer_security#cite_note-32) and [Sony Pictures](https://en.wikipedia.org/wiki/Sony_Pictures) [was attacked in 2014](https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack) where the motive appears to have been to embarrass with data leaks, and cripple the company by wiping workstations and servers.[[33]](https://en.wikipedia.org/wiki/Computer_security#cite_note-33)[[34]](https://en.wikipedia.org/wiki/Computer_security#cite_note-34)

**Automobiles**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=18)]

If access is gained to a car's internal [controller area network](https://en.wikipedia.org/wiki/Controller_area_network), it is possible to disable the brakes and turn the steering wheel.[[35]](https://en.wikipedia.org/wiki/Computer_security#cite_note-vox-35) Computerized engine timing, [cruise control](https://en.wikipedia.org/wiki/Cruise_control), [anti-lock brakes](https://en.wikipedia.org/wiki/Anti-lock_brakes), seat belt tensioners, door locks, [airbags](https://en.wikipedia.org/wiki/Airbag) and [advanced driver assistance systems](https://en.wikipedia.org/wiki/Advanced_driver_assistance_systems) make these disruptions possible, and [self-driving cars](https://en.wikipedia.org/wiki/Self-driving_car) go even further. [Connected cars](https://en.wikipedia.org/wiki/Connected_car) may use wifi and bluetooth to communicate with onboard consumer devices, and the cell phone network to contact concierge and emergency assistance services or get navigational or entertainment information; each of these networks is a potential entry point for malware or an attacker.[[35]](https://en.wikipedia.org/wiki/Computer_security#cite_note-vox-35) Researchers in 2011 were even able to use a malicious [compact disc](https://en.wikipedia.org/wiki/Compact_disc) in a car's stereo system as a successful attack vector,[[36]](https://en.wikipedia.org/wiki/Computer_security#cite_note-36) and cars with built-in voice recognition or remote assistance features have onboard microphones which could be used for eavesdropping.

A 2015 report by U.S. Senator Edward Markey criticized manufacturers' security measures as inadequate, and also highlighted privacy concerns about driving, location, and diagnostic data being collected, which is vulnerable to abuse by both manufacturers and hackers.[[37]](https://en.wikipedia.org/wiki/Computer_security#cite_note-37)

**Government**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=19)]

Government and [military](https://en.wikipedia.org/wiki/Military) computer systems are commonly attacked by activists[[38]](https://en.wikipedia.org/wiki/Computer_security#cite_note-38)[[39]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Tel_profile-39)[[40]](https://en.wikipedia.org/wiki/Computer_security#cite_note-bbcprofile-40)[[41]](https://en.wikipedia.org/wiki/Computer_security#cite_note-publications1-41) and foreign powers.[[42]](https://en.wikipedia.org/wiki/Computer_security#cite_note-42)[[43]](https://en.wikipedia.org/wiki/Computer_security#cite_note-npr-43)[[44]](https://en.wikipedia.org/wiki/Computer_security#cite_note-cnn-44)[[45]](https://en.wikipedia.org/wiki/Computer_security#cite_note-45) Local and regional government infrastructure such as [traffic light](https://en.wikipedia.org/wiki/Traffic_light) controls, police and intelligence agency communications, [personnel records](https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach), student records,[[46]](https://en.wikipedia.org/wiki/Computer_security#cite_note-46) and financial systems are also potential targets as they are now all largely computerized. [Passports](https://en.wikipedia.org/wiki/Passport) and government [ID cards](https://en.wikipedia.org/wiki/ID_card) that control access to facilities which use [RFID](https://en.wikipedia.org/wiki/RFID) can be vulnerable to [cloning](https://en.wikipedia.org/wiki/Phone_cloning).

**Internet of Things and physical vulnerabilities**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=20)]

The [Internet of Things](https://en.wikipedia.org/wiki/Internet_of_Things) (IoT) is the network of physical objects such as devices, vehicles, and buildings that are [embedded](https://en.wikipedia.org/wiki/Embedded_system) with [electronics](https://en.wikipedia.org/wiki/Electronics), [software](https://en.wikipedia.org/wiki/Software), [sensors](https://en.wikipedia.org/wiki/Sensor), and [network connectivity](https://en.wikipedia.org/wiki/Internet_access) that enables them to collect and exchange data[[47]](https://en.wikipedia.org/wiki/Computer_security#cite_note-47) – and concerns have been raised that this is being developed without appropriate consideration of the security challenges involved.[[48]](https://en.wikipedia.org/wiki/Computer_security#cite_note-48)[[49]](https://en.wikipedia.org/wiki/Computer_security#cite_note-49)

While the IoT creates opportunities for more direct integration of the physical world into computer-based systems,[[50]](https://en.wikipedia.org/wiki/Computer_security#cite_note-50)[[51]](https://en.wikipedia.org/wiki/Computer_security#cite_note-51) it also provides opportunities for misuse. In particular, as the Internet of Things spreads widely, cyber attacks are likely to become an increasingly physical (rather than simply virtual) threat.[[52]](https://en.wikipedia.org/wiki/Computer_security#cite_note-52) If a front door's lock is connected to the Internet, and can be locked/unlocked from a phone, then a criminal could enter the home at the press of a button from a stolen or hacked phone. People could stand to lose much more than their credit card numbers in a world controlled by IoT-enabled devices. Thieves have also used electronic means to circumvent non-Internet-connected hotel door locks.[[53]](https://en.wikipedia.org/wiki/Computer_security#cite_note-53)

[Medical devices](https://en.wikipedia.org/wiki/Medical_devices) have either been successfully attacked or had potentially deadly vulnerabilities demonstrated, including both in-hospital diagnostic equipment[[54]](https://en.wikipedia.org/wiki/Computer_security#cite_note-54) and implanted devices including [pacemakers](https://en.wikipedia.org/wiki/Pacemaker)[[55]](https://en.wikipedia.org/wiki/Computer_security#cite_note-55) and [insulin pumps](https://en.wikipedia.org/wiki/Insulin_pump).[[56]](https://en.wikipedia.org/wiki/Computer_security#cite_note-56)

Impact of security breaches[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=21)]

Serious financial damage has been caused by [security breaches](https://en.wikipedia.org/wiki/Security_breaches), but because there is no standard model for estimating the cost of an incident, the only data available is that which is made public by the organizations involved. "Several computer security consulting firms produce estimates of total worldwide losses attributable to [virus](https://en.wikipedia.org/wiki/Computer_virus) and [worm](https://en.wikipedia.org/wiki/Computer_worm) attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of covert attacks). The reliability of these estimates is often challenged; the underlying methodology is basically anecdotal."[[57]](https://en.wikipedia.org/wiki/Computer_security#cite_note-57)

However, reasonable estimates of the financial cost of security breaches can actually help organizations make rational investment decisions. According to the classic [Gordon-Loeb Model](https://en.wikipedia.org/wiki/Gordon-Loeb_Model) analyzing the optimal investment level in information security, one can conclude that the amount a firm spends to protect information should generally be only a small fraction of the expected loss (i.e., the [expected value](https://en.wikipedia.org/wiki/Expected_value) of the loss resulting from a cyber/information [security breach](https://en.wikipedia.org/wiki/Security_breach)).[[58]](https://en.wikipedia.org/wiki/Computer_security#cite_note-58)

Attacker motivation[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=22)]

As with [physical security](https://en.wikipedia.org/wiki/Physical_security), the motivations for breaches of computer security vary between attackers. Some are thrill-seekers or [vandals](https://en.wikipedia.org/wiki/Vandalism), others are activists or criminals looking for financial gain. State-sponsored attackers are now common and well resourced, but started with amateurs such as [Markus Hess](https://en.wikipedia.org/wiki/Markus_Hess) who hacked for the [KGB](https://en.wikipedia.org/wiki/KGB), as recounted by [Clifford Stoll](https://en.wikipedia.org/wiki/Clifford_Stoll), in [*The Cuckoo's Egg*](https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg).

A standard part of [threat modelling](https://en.wikipedia.org/wiki/Threat_modelling) for any particular system is to identify what might motivate an attack on that system, and who might be motivated to breach it. The level and detail of precautions will vary depending on the system to be secured. A home [personal computer](https://en.wikipedia.org/wiki/Personal_computer), [bank](https://en.wikipedia.org/wiki/Bank), and [classified](https://en.wikipedia.org/wiki/Classified_information) military [network](https://en.wikipedia.org/wiki/Computer_network) face very different threats, even when the underlying technologies in use are similar.

Computer protection (countermeasures)[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=23)]

In computer security a countermeasure is an action, device, procedure, or technique that reduces a [threat](https://en.wikipedia.org/wiki/Threat_(computer)), a [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)), or an [attack](https://en.wikipedia.org/wiki/Attack_(computing)) by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.[[59]](https://en.wikipedia.org/wiki/Computer_security#cite_note-rfc2828-59)[[60]](https://en.wikipedia.org/wiki/Computer_security#cite_note-CNSSI4009-60)[[61]](https://en.wikipedia.org/wiki/Computer_security#cite_note-61)

Some common countermeasures are listed in the following sections:

**Security by design**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=24)]

*Main article:*[*Secure by design*](https://en.wikipedia.org/wiki/Secure_by_design)

[Security by design](https://en.wikipedia.org/wiki/Secure_by_design), or alternately secure by design, means that the software has been designed from the ground up to be secure. In this case, security is considered as a main feature.

Some of the techniques in this approach include:

* The [principle of least privilege](https://en.wikipedia.org/wiki/Principle_of_least_privilege), where each part of the system has only the privileges that are needed for its function. That way even if an [attacker](https://en.wikipedia.org/wiki/Hacker_(computer_security)) gains access to that part, they have only limited access to the whole system.
* [Automated theorem proving](https://en.wikipedia.org/wiki/Automated_theorem_proving) to prove the correctness of crucial software subsystems.
* [Code reviews](https://en.wikipedia.org/wiki/Code_review) and [unit testing](https://en.wikipedia.org/wiki/Unit_testing), approaches to make modules more secure where formal correctness proofs are not possible.
* [Defense in depth](https://en.wikipedia.org/wiki/Defense_in_depth_(computing)), where the design is such that more than one subsystem needs to be violated to compromise the integrity of the system and the information it holds.
* Default secure settings, and design to "fail secure" rather than "fail insecure" (see [fail-safe](https://en.wikipedia.org/wiki/Fail-safe) for the equivalent in [safety engineering](https://en.wikipedia.org/wiki/Safety_engineering)). Ideally, a secure system should require a deliberate, conscious, knowledgeable and free decision on the part of legitimate authorities in order to make it insecure.
* [Audit trails](https://en.wikipedia.org/wiki/Audit_trail) tracking system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined. Storing audit trails remotely, where they can only be appended to, can keep intruders from covering their tracks.
* [Full disclosure](https://en.wikipedia.org/wiki/Full_disclosure_(computer_security)) of all vulnerabilities, to ensure that the "[window of vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing))" is kept as short as possible when bugs are discovered.

**Security architecture**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=25)]

The Open Security Architecture organization defines IT security architecture as "the design [artifacts](https://en.wikipedia.org/wiki/Artifact_(software_development)) that describe how the security controls (security countermeasures) are positioned, and how they relate to the overall information technology architecture. These controls serve the purpose to maintain the system's quality attributes: confidentiality, integrity, availability, accountability and [assurance services](https://en.wikipedia.org/wiki/Assurance_services)".[[62]](https://en.wikipedia.org/wiki/Computer_security#cite_note-62)

Techopedia defines security architecture as "a unified security design that addresses the necessities and potential risks involved in a certain scenario or environment. It also specifies when and where to apply security controls. The design process is generally reproducible." The key attributes of security architecture are:[[63]](https://en.wikipedia.org/wiki/Computer_security#cite_note-63)

* the relationship of different components and how they depend on each other.
* the determination of controls based on risk assessment, good practice, finances, and legal matters.
* the standardization of controls.

**Security measures**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=26)]

A state of computer "security" is the conceptual ideal, attained by the use of the three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

* [User account](https://en.wikipedia.org/wiki/User_account) [access controls](https://en.wikipedia.org/wiki/Access_control) and [cryptography](https://en.wikipedia.org/wiki/Cryptography) can protect systems files and data, respectively.
* [Firewalls](https://en.wikipedia.org/wiki/Firewall_(networking)) are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.
* [Intrusion Detection System](https://en.wikipedia.org/wiki/Intrusion_Detection_System) (IDS) products are designed to detect network attacks in-progress and assist in post-attack [forensics](https://en.wikipedia.org/wiki/Forensics), while [audit trails](https://en.wikipedia.org/wiki/Audit_trail) and [logs](https://en.wikipedia.org/wiki/Data_logging) serve a similar function for individual systems.
* "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of [legal](https://en.wikipedia.org/wiki/Legal) authorities, counter-attacks, and the like. In some special cases, a complete destruction of the compromised system is favored, as it may happen that not all the compromised resources are detected.

Today, computer security comprises mainly "preventive" measures, like firewalls or an [exit procedure](https://en.wikipedia.org/wiki/Exit_procedure). A firewall can be defined as a way of filtering network data between a host or a network and another network, such as the [Internet](https://en.wikipedia.org/wiki/Internet), and can be implemented as software running on the machine, hooking into the [network stack](https://en.wikipedia.org/wiki/Network_stack) (or, in the case of most [UNIX](https://en.wikipedia.org/wiki/UNIX)-based operating systems such as [Linux](https://en.wikipedia.org/wiki/Linux), built into the operating system [kernel](https://en.wikipedia.org/wiki/Kernel_(computer_science))) to provide real time filtering and blocking. Another implementation is a so-called "physical firewall", which consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the [Internet](https://en.wikipedia.org/wiki/Internet).

Some organizations are turning to [big data](https://en.wikipedia.org/wiki/Big_data) platforms, such as [Apache Hadoop](https://en.wikipedia.org/wiki/Apache_Hadoop), to extend data accessibility and [machine learning](https://en.wikipedia.org/wiki/Machine_learning) to detect [advanced persistent threats](https://en.wikipedia.org/wiki/Advanced_persistent_threat).[[64]](https://en.wikipedia.org/wiki/Computer_security#cite_note-64)[[65]](https://en.wikipedia.org/wiki/Computer_security#cite_note-65)

However, relatively few organisations maintain computer systems with effective detection systems, and fewer still have organised response mechanisms in place. As result, as Reuters points out: "Companies for the first time report they are losing more through electronic theft of data than physical stealing of assets".[[66]](https://en.wikipedia.org/wiki/Computer_security#cite_note-66) The primary obstacle to effective eradication of cyber crime could be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using [packet capture appliances](https://en.wikipedia.org/wiki/Packet_capture_appliance) that puts criminals behind bars.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Vulnerability management**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=27)]

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

Vulnerability management is the cycle of identifying, and remediating or mitigating [vulnerabilities](https://en.wikipedia.org/wiki/Software_vulnerability)",[[67]](https://en.wikipedia.org/wiki/Computer_security#cite_note-67) especially in [software](https://en.wikipedia.org/wiki/Software) and [firmware](https://en.wikipedia.org/wiki/Firmware). Vulnerability management is integral to computer security and [network security](https://en.wikipedia.org/wiki/Network_security).

Vulnerabilities can be discovered with a [vulnerability scanner](https://en.wikipedia.org/wiki/Vulnerability_scanner), which analyzes a computer system in search of known vulnerabilities,[[68]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Codenomicon-68) such as [open ports](https://en.wikipedia.org/wiki/Open_port), insecure software configuration, and susceptibility to [malware](https://en.wikipedia.org/wiki/Malware)

Beyond vulnerability scanning, many organisations contract outside security auditors to run regular [penetration tests](https://en.wikipedia.org/wiki/Penetration_test) against their systems to identify vulnerabilities. In some sectors this is a contractual requirement.[[69]](https://en.wikipedia.org/wiki/Computer_security#cite_note-69)

**Reducing vulnerabilities**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=28)]

While [formal verification](https://en.wikipedia.org/wiki/Formal_verification) of the correctness of computer systems is possible,[[70]](https://en.wikipedia.org/wiki/Computer_security#cite_note-70)[[71]](https://en.wikipedia.org/wiki/Computer_security#cite_note-71) it is not yet common. Operating systems formally verified include [seL4](https://en.wikipedia.org/wiki/SeL4),[[72]](https://en.wikipedia.org/wiki/Computer_security#cite_note-72) and [SYSGO](https://en.wikipedia.org/wiki/SYSGO)'s [PikeOS](https://en.wikipedia.org/wiki/PikeOS)[[73]](https://en.wikipedia.org/wiki/Computer_security#cite_note-73)[[74]](https://en.wikipedia.org/wiki/Computer_security#cite_note-74) – but these make up a very small percentage of the market.

[Cryptography](https://en.wikipedia.org/wiki/Cryptography) properly implemented is now virtually impossible to directly break. Breaking them requires some non-cryptographic input, such as a stolen key, stolen plaintext (at either end of the transmission), or some other extra cryptanalytic information.

[Two factor authentication](https://en.wikipedia.org/wiki/Two_factor_authentication) is a method for mitigating unauthorized access to a system or sensitive information. It requires "something you know"; a password or PIN, and "something you have"; a card, dongle, cellphone, or other piece of hardware. This increases security as an unauthorized person needs both of these to gain access.

Social engineering and direct computer access (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Training is often involved to help mitigate this risk,[[75]](https://en.wikipedia.org/wiki/Computer_security#cite_note-ALS14-75)[[76]](https://en.wikipedia.org/wiki/Computer_security#cite_note-SGA14-76) but even in a highly disciplined environments (e.g. military organizations), social engineering attacks can still be difficult to foresee and prevent.

It is possible to reduce an attacker's chances by keeping systems up to date with security patches and updates, using a security scanner or/and hiring competent people responsible for security. The effects of data loss/damage can be reduced by careful [backing up](https://en.wikipedia.org/wiki/Backup) and [insurance](https://en.wikipedia.org/wiki/Insurance).

**Hardware protection mechanisms**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=29)]

*See also:*[*Computer security compromised by hardware failure*](https://en.wikipedia.org/wiki/Computer_security_compromised_by_hardware_failure)

While hardware may be a source of insecurity, such as with microchip vulnerabilities maliciously introduced during the manufacturing process,[[77]](https://en.wikipedia.org/wiki/Computer_security#cite_note-77)[[78]](https://en.wikipedia.org/wiki/Computer_security#cite_note-78) hardware-based or assisted computer security also offers an alternative to software-only computer security. Using devices and methods such as [dongles](https://en.wikipedia.org/wiki/Dongle), [trusted platform modules](https://en.wikipedia.org/wiki/Trusted_platform_module), intrusion-aware cases, drive locks, disabling USB ports, and mobile-enabled access may be considered more secure due to the physical access (or sophisticated [backdoor access](https://en.wikipedia.org/wiki/Backdoor_(computing))) required in order to be compromised. Each of these is covered in more detail below.

* USB [dongles](https://en.wikipedia.org/wiki/Dongle) are typically used in software licensing schemes to unlock software capabilities,[[79]](https://en.wikipedia.org/wiki/Computer_security#cite_note-79) but they can also be seen as a way to prevent unauthorized access to a computer or other device's software. The dongle, or key, essentially creates a secure encrypted tunnel between the software application and the key. The principle is that an encryption scheme on the dongle, such as [Advanced Encryption Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) (AES) provides a stronger measure of security, since it is harder to hack and replicate the dongle than to simply copy the native software to another machine and use it. Another security application for dongles is to use them for accessing web-based content such as cloud software or [Virtual Private Networks](https://en.wikipedia.org/wiki/Virtual_Private_Networks) (VPNs).[[80]](https://en.wikipedia.org/wiki/Computer_security#cite_note-80) In addition, a USB dongle can be configured to lock or unlock a computer.[[81]](https://en.wikipedia.org/wiki/Computer_security#cite_note-81)
* [Trusted platform modules](https://en.wikipedia.org/wiki/Trusted_platform_module) (TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.[[82]](https://en.wikipedia.org/wiki/Computer_security#cite_note-82)
* [Computer case intrusion detection](https://en.wikipedia.org/wiki/Computer_case#Intrusion_detection) refers to a push-button switch which is triggered when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.
* Drive locks are essentially software tools to encrypt hard drives, making them inaccessible to thieves.[[83]](https://en.wikipedia.org/wiki/Computer_security#cite_note-83) Tools exist specifically for encrypting external drives as well.[[84]](https://en.wikipedia.org/wiki/Computer_security#cite_note-84)
* Disabling USB ports is a security option for preventing unauthorized and malicious access to an otherwise secure computer. Infected USB dongles connected to a network from a computer inside the firewall are considered by the magazine Network World as the most common hardware threat facing computer networks.[[85]](https://en.wikipedia.org/wiki/Computer_security#cite_note-85)
* Mobile-enabled access devices are growing in popularity due to the ubiquitous nature of cell phones. Built-in capabilities such as [Bluetooth](https://en.wikipedia.org/wiki/Bluetooth), the newer [Bluetooth low energy](https://en.wikipedia.org/wiki/Bluetooth_low_energy)(LE), [Near field communication](https://en.wikipedia.org/wiki/Near_field_communication) (NFC) on non-iOS devices and [biometric](https://en.wikipedia.org/wiki/Biometrics) validation such as thumb print readers, as well as [QR code](https://en.wikipedia.org/wiki/QR_code) reader software designed for mobile devices, offer new, secure ways for mobile phones to connect to access control systems. These control systems provide computer security and can also be used for controlling access to secure buildings.[[86]](https://en.wikipedia.org/wiki/Computer_security#cite_note-86)

**Secure operating systems**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=30)]

*Main article:*[*Security-evaluated operating system*](https://en.wikipedia.org/wiki/Security-evaluated_operating_system)

One use of the term "computer security" refers to technology that is used to implement secure [operating systems](https://en.wikipedia.org/wiki/Operating_system). In the 1980s the [United States](https://en.wikipedia.org/wiki/United_States) [Department of Defense](https://en.wikipedia.org/wiki/United_States_Department_of_Defense) (DoD) used the ["Orange Book"](https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria)[[87]](https://en.wikipedia.org/wiki/Computer_security#cite_note-87) standards, but the current international standard ISO/IEC 15408, "[Common Criteria](https://en.wikipedia.org/wiki/Common_Criteria)" defines a number of progressively more stringent [Evaluation Assurance Levels](https://en.wikipedia.org/wiki/Evaluation_Assurance_Level). Many common operating systems meet the EAL4 standard of being "Methodically Designed, Tested and Reviewed", but the [formal verification](https://en.wikipedia.org/wiki/Formal_verification) required for the highest levels means that they are uncommon. An example of an EAL6 ("Semiformally Verified Design and Tested") system is [Integrity-178B](https://en.wikipedia.org/wiki/INTEGRITY-178B), which is used in the [Airbus A380](https://en.wikipedia.org/wiki/Airbus_A380)[[88]](https://en.wikipedia.org/wiki/Computer_security#cite_note-darkreading-88)and several military jets.[[89]](https://en.wikipedia.org/wiki/Computer_security#cite_note-VITA_Technologies_Magazine-89)

**Secure coding**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=31)]

*Main article:*[*Secure coding*](https://en.wikipedia.org/wiki/Secure_coding)

In software engineering, [secure coding](https://en.wikipedia.org/wiki/Secure_coding) aims to guard against the accidental introduction of security vulnerabilities. It is also possible to create software designed from the ground up to be secure. Such systems are "[secure by design](https://en.wikipedia.org/wiki/Secure_by_design)". Beyond this, [formal verification](https://en.wikipedia.org/wiki/Formal_verification) aims to prove the [correctness](https://en.wikipedia.org/wiki/Correctness_(computer_science)) of the [algorithms](https://en.wikipedia.org/wiki/Algorithms) underlying a system;[[90]](https://en.wikipedia.org/wiki/Computer_security#cite_note-90) important for [cryptographic protocols](https://en.wikipedia.org/wiki/Cryptographic_protocol) for example.

**Capabilities and access control lists**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=32)]

*Main articles:*[*Access control list*](https://en.wikipedia.org/wiki/Access_control_list)*and*[*Capability (computers)*](https://en.wikipedia.org/wiki/Capability_(computers))

Within computer systems, two of many [security models](https://en.wikipedia.org/wiki/Computer_security_model) capable of enforcing privilege separation are [access control lists](https://en.wikipedia.org/wiki/Access_control_list) (ACLs) and [capability-based security](https://en.wikipedia.org/wiki/Capability-based_security). Using ACLs to confine programs has been proven to be insecure in many situations, such as if the host computer can be tricked into indirectly allowing restricted file access, an issue known as the [confused deputy problem](https://en.wikipedia.org/wiki/Confused_deputy_problem). It has also been shown that the promise of ACLs of giving access to an object to only one person can never be guaranteed in practice. Both of these problems are resolved by capabilities. This does not mean practical flaws exist in all ACL-based systems, but only that the designers of certain utilities must take responsibility to ensure that they do not introduce flaws.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Capabilities have been mostly restricted to research [operating systems](https://en.wikipedia.org/wiki/Operating_system), while commercial OSs still use ACLs. Capabilities can, however, also be implemented at the language level, leading to a style of programming that is essentially a refinement of standard object-oriented design. An open source project in the area is the [E language](https://en.wikipedia.org/wiki/E_programming_language).

The most secure computers are those not connected to the Internet and shielded from any interference. In the real world, the most secure systems are [operating systems](https://en.wikipedia.org/wiki/Operating_system) where [security](https://en.wikipedia.org/wiki/Security) is not an add-on.

**Response to breaches**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=33)]

Responding forcefully to attempted [security breaches](https://en.wikipedia.org/wiki/Security_breaches) (in the manner that one would for attempted physical security breaches) is often very difficult for a variety of reasons:

* Identifying attackers is difficult, as they are often in a different [jurisdiction](https://en.wikipedia.org/wiki/Jurisdiction) to the systems they attempt to breach, and operate through proxies, temporary anonymous dial-up accounts, wireless connections, and other anonymising procedures which make backtracing difficult and are often located in yet another jurisdiction. If they successfully breach security, they are often able to delete [logs](https://en.wikipedia.org/wiki/Data_logging) to cover their tracks.
* The sheer number of attempted attacks is so large that organisations cannot spend time pursuing each attacker (a typical home user with a permanent (e.g., [cable modem](https://en.wikipedia.org/wiki/Cable_modem)) connection will be attacked at least several times per day, so more attractive targets could be presumed to see many more). Note however, that most of the sheer bulk of these attacks are made by automated [vulnerability scanners](https://en.wikipedia.org/wiki/Vulnerability_scanner) and [computer worms](https://en.wikipedia.org/wiki/Computer_worm).
* [Law enforcement officers](https://en.wikipedia.org/wiki/Law_enforcement_officer) are often unfamiliar with [information technology](https://en.wikipedia.org/wiki/Information_technology), and so lack the skills and interest in pursuing attackers. There are also budgetary constraints. It has been argued that the high cost of technology, such as [DNA](https://en.wikipedia.org/wiki/DNA) testing, and improved [forensics](https://en.wikipedia.org/wiki/Forensics) mean less money for other kinds of law enforcement, so the overall rate of criminals not getting dealt with goes up as the cost of the technology increases. In addition, the identification of attackers across a network may require logs from various points in the network and in many countries, the release of these records to law enforcement (with the exception of being voluntarily surrendered by a [network administrator](https://en.wikipedia.org/wiki/Network_administrator)or a [system administrator](https://en.wikipedia.org/wiki/System_administrator)) requires a [search warrant](https://en.wikipedia.org/wiki/Search_warrant) and, depending on the circumstances, the legal proceedings required can be drawn out to the point where the records are either regularly destroyed, or the information is no longer relevant.

Notable attacks and breaches[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=34)]

*Further information:*[*List of cyber-attacks*](https://en.wikipedia.org/wiki/List_of_cyber-attacks)

Some illustrative examples of different types of computer security breaches are given below.

**Robert Morris and the first computer worm**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=35)]

*Main article:*[*Morris worm*](https://en.wikipedia.org/wiki/Morris_worm)

In 1988, only 60,000 computers were connected to the Internet, and most were mainframes, minicomputers and professional workstations. On November 2, 1988, many started to slow down, because they were running a malicious code that demanded processor time and that spread itself to other computers – the first internet "[computer worm](https://en.wikipedia.org/wiki/Computer_worm)".[[91]](https://en.wikipedia.org/wiki/Computer_security#cite_note-multiple-91) The software was traced back to 23-year-old [Cornell University](https://en.wikipedia.org/wiki/Cornell_University) graduate student [Robert Tappan Morris, Jr.](https://en.wikipedia.org/wiki/Robert_Tappan_Morris,_Jr.) who said 'he wanted to count how many machines were connected to the Internet'.[[91]](https://en.wikipedia.org/wiki/Computer_security#cite_note-multiple-91)

**Rome Laboratory**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=36)]

In 1994, over a hundred intrusions were made by unidentified crackers into the [Rome Laboratory](https://en.wikipedia.org/wiki/Rome_Laboratory), the US Air Force's main command and research facility. Using [trojan horses](https://en.wikipedia.org/wiki/Trojan_horse_(computing)), hackers were able to obtain unrestricted access to Rome's networking systems and remove traces of their activities. The intruders were able to obtain classified files, such as air tasking order systems data and furthermore able to penetrate connected networks of [National Aeronautics and Space Administration](https://en.wikipedia.org/wiki/National_Aeronautics_and_Space_Administration)'s Goddard Space Flight Center, Wright-Patterson Air Force Base, some Defense contractors, and other private sector organizations, by posing as a trusted Rome center user.[[92]](https://en.wikipedia.org/wiki/Computer_security#cite_note-92)

**TJX customer credit card details**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=37)]

In early 2007, American apparel and home goods company [TJX](https://en.wikipedia.org/wiki/TJX_Companies) announced that it was the victim of an [unauthorized computer systems intrusion](https://en.wikipedia.org/wiki/Hacker_(computer_security))[[93]](https://en.wikipedia.org/wiki/Computer_security#cite_note-93) and that the hackers had accessed a system that stored data on [credit card](https://en.wikipedia.org/wiki/Credit_card), [debit card](https://en.wikipedia.org/wiki/Debit_card), [check](https://en.wikipedia.org/wiki/Cheque), and merchandise return transactions.[[94]](https://en.wikipedia.org/wiki/Computer_security#cite_note-94)

**Stuxnet attack**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=38)]

The computer worm known as [Stuxnet](https://en.wikipedia.org/wiki/Stuxnet) reportedly ruined almost one-fifth of Iran's [nuclear centrifuges](https://en.wikipedia.org/wiki/Nuclear_centrifuge)[[95]](https://en.wikipedia.org/wiki/Computer_security#cite_note-95) by disrupting industrial [programmable logic controllers](https://en.wikipedia.org/wiki/Programmable_logic_controller) (PLCs) in a targeted attack generally believed to have been launched by Israel and the United States[[96]](https://en.wikipedia.org/wiki/Computer_security#cite_note-us-96)[[97]](https://en.wikipedia.org/wiki/Computer_security#cite_note-97)[[98]](https://en.wikipedia.org/wiki/Computer_security#cite_note-98)[[99]](https://en.wikipedia.org/wiki/Computer_security#cite_note-99) although neither has publicly acknowledged this.

**Global surveillance disclosures**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=39)]

*Main article:*[*Global surveillance disclosures (2013–present)*](https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present))

In early 2013, massive breaches of computer security by the [NSA](https://en.wikipedia.org/wiki/NSA) were revealed, including deliberately inserting a backdoor in a [NIST](https://en.wikipedia.org/wiki/NIST) standard for encryption[[100]](https://en.wikipedia.org/wiki/Computer_security#cite_note-100) and tapping the links between [Google](https://en.wikipedia.org/wiki/Google)'s data centres.[[101]](https://en.wikipedia.org/wiki/Computer_security#cite_note-101) These were disclosed by [NSA](https://en.wikipedia.org/wiki/NSA) contractor [Edward Snowden](https://en.wikipedia.org/wiki/Edward_Snowden).[[102]](https://en.wikipedia.org/wiki/Computer_security#cite_note-ARDinterview-102)

**Target and Home Depot breaches**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=40)]

In 2013 and 2014, a [Russian](https://en.wikipedia.org/wiki/Russia)/[Ukrainian](https://en.wikipedia.org/wiki/Ukraine) hacking ring known as "Rescator" broke into [Target Corporation](https://en.wikipedia.org/wiki/Target_Corporation) computers in 2013, stealing roughly 40 million credit cards,[[103]](https://en.wikipedia.org/wiki/Computer_security#cite_note-103) and then [Home Depot](https://en.wikipedia.org/wiki/Home_Depot) computers in 2014, stealing between 53 and 56 million credit card numbers.[[104]](https://en.wikipedia.org/wiki/Computer_security#cite_note-104) Warnings were delivered at both corporations, but ignored; physical security breaches using [self checkout machines](https://en.wikipedia.org/wiki/Self-checkout) are believed to have played a large role. "The malware utilized is absolutely unsophisticated and uninteresting," says Jim Walter, director of threat intelligence operations at security technology company McAfee – meaning that the heists could have easily been stopped by existing [antivirus](https://en.wikipedia.org/wiki/Antivirus) software had administrators responded to the warnings. The size of the thefts has resulted in major attention from state and Federal United States authorities and the investigation is ongoing.

**Ashley Madison breach**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=41)]

*Main article:*[*Ashley Madison Data Breach*](https://en.wikipedia.org/wiki/Ashley_Madison_data_breach)

In July 2015, a hacker group known as "The Impact Team" successfully breached the extramarital relationship website Ashley Madison. The group claimed that they had taken not only company data but user data as well. After the breach, The Impact Team dumped emails from the company's CEO, to prove their point, and threatened to dump customer data unless the website was taken down permanently. With this initial data release, the group stated "[Avid Life Media](https://en.wikipedia.org/wiki/Avid_Life_Media) has been instructed to take Ashley Madison and Established Men offline permanently in all forms, or we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails. The other websites may stay online."[[105]](https://en.wikipedia.org/wiki/Computer_security#cite_note-105) When Avid Life Media, the parent company that created the Ashley Madison website, did not take the site offline, The Impact Group released two more compressed files, one 9.7GB and the second 20GB. After the second data dump, Avid Life Media CEO Noel Biderman resigned, but the website remained functional.

Legal issues and global regulation[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=42)]

Conflict of laws in cyberspace has become a major cause of concern for computer security community. Some of the main challenges and complaints about the antivirus industry are the lack of global web regulations, a global base of common rules to judge, and eventually punish, [cyber crimes](https://en.wikipedia.org/wiki/Cybercrime) and cyber criminals. There is no global cyber law and cybersecurity treaty that can be invoked for enforcing global cybersecurity issues.

International legal issues of cyber attacks are complicated in nature. Even if an antivirus firm locates the cyber criminal behind the creation of a particular [virus](https://en.wikipedia.org/wiki/Virus_(computer)) or piece of [malware](https://en.wikipedia.org/wiki/Malware) or form of [cyber attack](https://en.wikipedia.org/wiki/Cyber-Attacks), often the local authorities cannot take action due to lack of laws under which to prosecute.[[106]](https://en.wikipedia.org/wiki/Computer_security#cite_note-ted.com-106)[[107]](https://en.wikipedia.org/wiki/Computer_security#cite_note-107) Authorship attribution for cyber crimes and cyber attacks is a major problem for all law enforcement agencies.

"[Computer viruses] switch from one country to another, from one jurisdiction to another – moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone [had] given free plane tickets to all the online criminals of the world."[[106]](https://en.wikipedia.org/wiki/Computer_security#cite_note-ted.com-106) Use of [dynamic DNS](https://en.wikipedia.org/wiki/Dynamic_DNS), [fast flux](https://en.wikipedia.org/wiki/Fast_flux) and [bullet proof servers](https://en.wikipedia.org/wiki/Bulletproof_hosting) have added own complexities to this situation.

Government[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=43)]

The role of the government is to make [regulations](https://en.wikipedia.org/wiki/Cyber-security_regulation) to force companies and organizations to protect their systems, infrastructure and information from any [cyber-attacks](https://en.wikipedia.org/wiki/Cyber-attack), but also to protect its own national infrastructure such as the national [power-grid](https://en.wikipedia.org/wiki/Power_grid).[[108]](https://en.wikipedia.org/wiki/Computer_security#cite_note-108)

The question of whether the government should intervene or not in the regulation of the [cyberspace](https://en.wikipedia.org/wiki/Cyberspace) is a very polemical one. Indeed, for as long as it has existed and by definition, the cyberspace is a [virtual space](https://en.wikipedia.org/wiki/Virtual_space) free of any government intervention. Where everyone agree that an improvement on cybersecurity is more than vital, is the government the best actor to solve this issue? Many government officials and experts think that the government should step in and that there is a crucial need for regulation, mainly due to the failure of the private sector to solve efficiently the cybersecurity problem. [R. Clarke](https://en.wikipedia.org/wiki/Richard_A._Clarke) said during a panel discussion at the [RSA Security Conference](https://en.wikipedia.org/wiki/RSA_Conference) in [San Francisco](https://en.wikipedia.org/wiki/San_Francisco), he believes that the "industry only responds when you threaten regulation. If industry doesn't respond (to the threat), you have to follow through."[[109]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Clarke_ref-109) On the other hand, executives from the private sector agree that improvements are necessary, but think that the government intervention would affect their ability to innovate efficiently.

Actions and teams in the US[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=44)]

**Legislation**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=45)]

The 1986 [18 U.S.C.](https://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code) [§ 1030](https://www.law.cornell.edu/uscode/text/18/1030), more commonly known as the [Computer Fraud and Abuse Act](https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act) is the key legislation. It prohibits unauthorized access or damage of "protected computers" as defined in [18 U.S.C.](https://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code) [§ 1030(e)(2)](https://www.law.cornell.edu/uscode/text/18/1030#e_2).

Although various other measures have been proposed, such as the "Cybersecurity Act of 2010 – S. 773" in 2009, the "International Cybercrime Reporting and Cooperation Act – H.R.4962"[[110]](https://en.wikipedia.org/wiki/Computer_security#cite_note-110) and "Protecting Cyberspace as a National Asset Act of 2010 – S.3480"[[111]](https://en.wikipedia.org/wiki/Computer_security#cite_note-111) in 2010 – none of these has succeeded.

[Executive order](https://en.wikipedia.org/wiki/Executive_order) [13636](https://en.wikisource.org/wiki/Executive_Order_13636) *Improving Critical Infrastructure Cybersecurity* was signed February 12, 2013.

**Agencies**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=46)]

The [Department of Homeland Security](https://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security) has a dedicated division responsible for the response system, [risk management](https://en.wikipedia.org/wiki/Risk_management) program and requirements for cybersecurity in the United States called the [National Cyber Security Division](https://en.wikipedia.org/wiki/National_Cyber_Security_Division).[[112]](https://en.wikipedia.org/wiki/Computer_security#cite_note-112)[[113]](https://en.wikipedia.org/wiki/Computer_security#cite_note-CSRDC-FAQ-113) The division is home to US-CERT operations and the National Cyber Alert System.[[113]](https://en.wikipedia.org/wiki/Computer_security#cite_note-CSRDC-FAQ-113) The National Cybersecurity and Communications Integration Center brings together government organizations responsible for protecting computer networks and networked infrastructure.[[114]](https://en.wikipedia.org/wiki/Computer_security#cite_note-114)

The third priority of the [Federal Bureau of Investigation](https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation) (FBI) is to: *"Protect the United States against cyber-based attacks and high-technology crimes"*,[[115]](https://en.wikipedia.org/wiki/Computer_security#cite_note-priorities-115) and they, along with the [National White Collar Crime Center](https://en.wikipedia.org/wiki/National_White_Collar_Crime_Center) (NW3C), and the [Bureau of Justice Assistance](https://en.wikipedia.org/wiki/Bureau_of_Justice_Assistance) (BJA) are part of the multi-agency task force, The [Internet Crime Complaint Center](https://en.wikipedia.org/wiki/Internet_Crime_Complaint_Center), also known as IC3.[[116]](https://en.wikipedia.org/wiki/Computer_security#cite_note-ic3-116)

In addition to its own specific duties, the FBI participates alongside non-profit organizations such as [InfraGard](https://en.wikipedia.org/wiki/InfraGard).[[117]](https://en.wikipedia.org/wiki/Computer_security#cite_note-infragard-site-117)[[118]](https://en.wikipedia.org/wiki/Computer_security#cite_note-mueller-video-118)

In the [criminal division](https://en.wikipedia.org/wiki/United_States_Department_of_Justice_Criminal_Division) of the [United States Department of Justice](https://en.wikipedia.org/wiki/United_States_Department_of_Justice) operates a section called the [Computer Crime and Intellectual Property Section](https://en.wikipedia.org/wiki/Computer_Crime_and_Intellectual_Property_Section). The CCIPS is in charge of investigating [computer crime](https://en.wikipedia.org/wiki/Computer_crime) and [intellectual property](https://en.wikipedia.org/wiki/Intellectual_property) crime and is specialized in the search and seizure of [digital evidence](https://en.wikipedia.org/wiki/Digital_evidence) in computers and [networks](https://en.wikipedia.org/wiki/Computer_network).[[119]](https://en.wikipedia.org/wiki/Computer_security#cite_note-CCIPS-119)

The [United States Cyber Command](https://en.wikipedia.org/wiki/USCYBERCOM), also known as USCYBERCOM, is tasked with the defense of specified Department of Defense information networks and *"ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."*[[120]](https://en.wikipedia.org/wiki/Computer_security#cite_note-120) It has no role in the protection of civilian networks.[[121]](https://en.wikipedia.org/wiki/Computer_security#cite_note-121)[[122]](https://en.wikipedia.org/wiki/Computer_security#cite_note-122)

The U.S. [Federal Communications Commission](https://en.wikipedia.org/wiki/Federal_Communications_Commission)'s role in cybersecurity is to strengthen the protection of critical communications infrastructure, to assist in maintaining the reliability of networks during disasters, to aid in swift recovery after, and to ensure that first responders have access to effective communications services.[[123]](https://en.wikipedia.org/wiki/Computer_security#cite_note-FCC-123)

The [Food and Drug Administration](https://en.wikipedia.org/wiki/Food_and_Drug_Administration) has issued guidance for medical devices,[[124]](https://en.wikipedia.org/wiki/Computer_security#cite_note-124) and the [National Highway Traffic Safety Administration](https://en.wikipedia.org/wiki/National_Highway_Traffic_Safety_Administration)[[125]](https://en.wikipedia.org/wiki/Computer_security#cite_note-125) is concerned with automotive cybersecurity. After being criticized by the [Government Accountability Office](https://en.wikipedia.org/wiki/Government_Accountability_Office),[[126]](https://en.wikipedia.org/wiki/Computer_security#cite_note-126) and following successful attacks on airports and claimed attacks on airplanes, the [Federal Aviation Administration](https://en.wikipedia.org/wiki/Federal_Aviation_Administration) has devoted funding to securing systems on board the planes of private manufacturers, and the [Aircraft Communications Addressing and Reporting System](https://en.wikipedia.org/wiki/Aircraft_Communications_Addressing_and_Reporting_System).[[127]](https://en.wikipedia.org/wiki/Computer_security#cite_note-127) Concerns have also been raised about the future [Next Generation Air Transportation System](https://en.wikipedia.org/wiki/Next_Generation_Air_Transportation_System).[[128]](https://en.wikipedia.org/wiki/Computer_security#cite_note-128)

**Computer emergency readiness team**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=47)]

"[Computer emergency response team](https://en.wikipedia.org/wiki/Computer_emergency_response_team)" is a name given to expert groups that handle computer security incidents. In the US, two distinct organization exist, although they do work closely together.

* [US-CERT](https://en.wikipedia.org/wiki/US-CERT): part of the [National Cyber Security Division](https://en.wikipedia.org/wiki/National_Cyber_Security_Division) of the [United States Department of Homeland Security](https://en.wikipedia.org/wiki/United_States_Department_of_Homeland_Security).[[129]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Computerworld-129)
* [CERT/CC](https://en.wikipedia.org/wiki/CERT_Coordination_Center): created by the [Defense Advanced Research Projects Agency](https://en.wikipedia.org/wiki/Defense_Advanced_Research_Projects_Agency) (DARPA) and run by the [Software Engineering Institute](https://en.wikipedia.org/wiki/Software_Engineering_Institute) (SEI).

International actions[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=48)]

Many different teams and organisations exist, including:

* The Forum of Incident Response and Security Teams (FIRST) is the global association of CSIRTs.[[130]](https://en.wikipedia.org/wiki/Computer_security#cite_note-FIRST-130) The [US-CERT](https://en.wikipedia.org/wiki/US-CERT), [AT&T](https://en.wikipedia.org/wiki/AT%26T), [Apple](https://en.wikipedia.org/wiki/Apple_Inc.), [Cisco](https://en.wikipedia.org/wiki/Cisco), [McAfee](https://en.wikipedia.org/wiki/McAfee), [Microsoft](https://en.wikipedia.org/wiki/Microsoft) are all members of this international team.[[131]](https://en.wikipedia.org/wiki/Computer_security#cite_note-FIRST_members-131)
* The [Council of Europe](https://en.wikipedia.org/wiki/Council_of_Europe) helps protect societies worldwide from the threat of cybercrime through the Convention on Cybercrime.[[132]](https://en.wikipedia.org/wiki/Computer_security#cite_note-European_council-132)
* The purpose of the [Messaging Anti-Abuse Working Group](https://en.wikipedia.org/wiki/Messaging_Anti-Abuse_Working_Group) (MAAWG) is to bring the messaging industry together to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations.[[133]](https://en.wikipedia.org/wiki/Computer_security#cite_note-MAAWG-133) [France Telecom](https://en.wikipedia.org/wiki/France_T%C3%A9l%C3%A9com), [Facebook](https://en.wikipedia.org/wiki/Facebook), [AT&T](https://en.wikipedia.org/wiki/AT%26T), [Apple](https://en.wikipedia.org/wiki/Apple_Inc.), [Cisco](https://en.wikipedia.org/wiki/Cisco), [Sprint](https://en.wikipedia.org/wiki/Sprint_Nextel) are some of the members of the MAAWG.[[134]](https://en.wikipedia.org/wiki/Computer_security#cite_note-MAAWGroster-134)
* ENISA : The [European Network and Information Security Agency](https://en.wikipedia.org/wiki/European_Network_and_Information_Security_Agency) (ENISA) is an [agency of the European Union](https://en.wikipedia.org/wiki/Agency_of_the_European_Union) with the objective to improve network and [information security](https://en.wikipedia.org/wiki/Information_security)in the [European Union](https://en.wikipedia.org/wiki/European_Union).

**Europe**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=49)]

CSIRTs in Europe collaborate in the [TERENA](https://en.wikipedia.org/wiki/TERENA) task force TF-CSIRT. [TERENA](https://en.wikipedia.org/wiki/TERENA)'s Trusted Introducer service provides an accreditation and certification scheme for CSIRTs in Europe. A full list of known CSIRTs in Europe is available from the Trusted Introducer website.

National teams[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=50)]

Here are the main [computer emergency response teams](https://en.wikipedia.org/wiki/Computer_emergency_response_team) around the world. Most countries have their own team to protect network security.

**Canada**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=51)]

On October 3, 2010, Public Safety Canada unveiled Canada's Cyber Security Strategy, following a Speech from the Throne commitment to boost the security of Canadian cyberspace.[[135]](https://en.wikipedia.org/wiki/Computer_security#cite_note-135)[[136]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Canada.27s_Cyber_Security_Strategy-136) The aim of the strategy is to strengthen Canada's "cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world."[[136]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Canada.27s_Cyber_Security_Strategy-136) Three main pillars define the strategy: securing government systems, partnering to secure vital cyber systems outside the federal government, and helping Canadians to be secure online.[[136]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Canada.27s_Cyber_Security_Strategy-136) The strategy involves multiple departments and agencies across the Government of Canada.[[137]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Government_of_Canada-137) The Cyber Incident Management Framework for Canada outlines these responsibilities, and provides a plan for coordinated response between government and other partners in the event of a cyber incident.[[138]](https://en.wikipedia.org/wiki/Computer_security#cite_note-138) The Action Plan 2010–2015 for Canada's Cyber Security Strategy outlines the ongoing implementation of the strategy.[[139]](https://en.wikipedia.org/wiki/Computer_security#cite_note-139)

Public Safety Canada's [Canadian Cyber Incident Response Centre](https://en.wikipedia.org/wiki/Canadian_Cyber_Incident_Response_Centre) (CCIRC) is responsible for mitigating and responding to threats to Canada's critical infrastructure and cyber systems. The CCIRC provides support to mitigate cyber threats, technical support to respond and recover from targeted cyber attacks, and provides online tools for members of Canada's critical infrastructure sectors.[[140]](https://en.wikipedia.org/wiki/Computer_security#cite_note-140) The CCIRC posts regular cyber security bulletins on the Public Safety Canada website.[[141]](https://en.wikipedia.org/wiki/Computer_security#cite_note-141) The CCIRC also operates an online reporting tool where individuals and organizations can report a cyber incident.[[142]](https://en.wikipedia.org/wiki/Computer_security#cite_note-142) Canada's Cyber Security Strategy is part of a larger, integrated approach to critical infrastructure protection, and functions as a counterpart document to the National Strategy and Action Plan for Critical Infrastructure.[[137]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Government_of_Canada-137)

On September 27, 2010, Public Safety Canada partnered with STOP.THINK.CONNECT, a coalition of non-profit, private sector, and government organizations dedicated to informing the general public on how to protect themselves online.[[143]](https://en.wikipedia.org/wiki/Computer_security#cite_note-143) On February 4, 2014, the Government of Canada launched the Cyber Security Cooperation Program.[[144]](https://en.wikipedia.org/wiki/Computer_security#cite_note-144)The program is a $1.5 million five-year initiative aimed at improving Canada's cyber systems through grants and contributions to projects in support of this objective.[[145]](https://en.wikipedia.org/wiki/Computer_security#cite_note-145) Public Safety Canada aims to begin an evaluation of Canada's Cyber Security Strategy in early 2015.[[137]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Government_of_Canada-137) Public Safety Canada administers and routinely updates the GetCyberSafe portal for Canadian citizens, and carries out Cyber Security Awareness Month during October.[[146]](https://en.wikipedia.org/wiki/Computer_security#cite_note-146)

**China**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=52)]

China's network security and information technology leadership team was established February 27, 2014. The leadership team is tasked with national security and long-term development and co-ordination of major issues related to network security and information technology. Economic, political, cultural, social and military fields as related to network security and information technology strategy, planning and major macroeconomic policy are being researched. The promotion of national network security and information technology law are constantly under study for enhanced national security capabilities.

**Germany**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=53)]

Berlin starts National Cyber Defense Initiative: On June 16, 2011, the German Minister for Home Affairs, officially opened the new German NCAZ (National Center for Cyber Defense) [Nationales Cyber-Abwehrzentrum](https://en.wikipedia.org/wiki/National_Cyberdefence_Centre) located in Bonn. The NCAZ closely cooperates with BSI (Federal Office for Information Security) [Bundesamt für Sicherheit in der Informationstechnik](https://en.wikipedia.org/wiki/Federal_Office_for_Information_Security), BKA (Federal Police Organisation) [Bundeskriminalamt (Deutschland)](https://en.wikipedia.org/wiki/Federal_Criminal_Police_Office_(Germany)), BND (Federal Intelligence Service) [Bundesnachrichtendienst](https://en.wikipedia.org/wiki/Bundesnachrichtendienst), MAD (Military Intelligence Service) [Amt für den Militärischen Abschirmdienst](https://en.wikipedia.org/wiki/Milit%C3%A4rischer_Abschirmdienst) and other national organisations in Germany taking care of national security aspects. According to the Minister the primary task of the new organisation founded on February 23, 2011, is to detect and prevent attacks against the national infrastructure and mentioned incidents like [Stuxnet](https://en.wikipedia.org/wiki/Stuxnet).

**India**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=54)]

Some provisions for cybersecurity have been incorporated into rules framed under the Information Technology Act 2000.

The [National Cyber Security Policy 2013](https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013) is a policy framework by Department of Electronics and Information Technology (DeitY) which aims to protect the public and private infrastructure from cyber attacks, and safeguard "information, such as personal information (of web users), financial and banking information and sovereign data".

The [Indian Companies Act 2013](https://en.wikipedia.org/w/index.php?title=Indian_Companies_Act_2013&action=edit&redlink=1) has also introduced cyber law and cyber security obligations on the part of Indian directors.

**Pakistan**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=55)]

Cyber-crime has risen rapidly in Pakistan. There are about 34 million Internet users with 133.4 million mobile subscribers in Pakistan. According to Cyber Crime Unit (CCU), a branch of Federal Investigation Agency, only 62 cases were reported to the unit in 2007, 287 cases in 2008, ratio dropped in 2009 but in 2010, more than 312 cases were registered. However, there are many unreported incidents of cyber-crime.[[147]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Tier3-147)

"Pakistan's Cyber Crime Bill 2007", the first pertinent law, focuses on electronic crimes, for example cyber-terrorism, criminal access, electronic system fraud, electronic forgery, and misuse of encryption.[[147]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Tier3-147)

National Response Centre for Cyber Crime (NR3C) – FIA is a law enforcement agency dedicated to fight cybercrime. Inception of this Hi-Tech crime fighting unit transpired in 2007 to identify and curb the phenomenon of technological abuse in society.[[148]](https://en.wikipedia.org/wiki/Computer_security#cite_note-148) However, certain private firms are also working in cohesion with the government to improve cyber security and curb cyberattacks.[[149]](https://en.wikipedia.org/wiki/Computer_security#cite_note-149)

**South Korea**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=56)]

Following cyberattacks in the first half of 2013, when government, news-media, television station, and bank websites were compromised, the national government committed to the training of 5,000 new cybersecurity experts by 2017. The South Korean government blamed its northern counterpart for these attacks, as well as incidents that occurred in 2009, 2011,[[150]](https://en.wikipedia.org/wiki/Computer_security#cite_note-South_Korean_news_agency_Yonhap-150) and 2012, but Pyongyang denies the accusations.[[151]](https://en.wikipedia.org/wiki/Computer_security#cite_note-Jun-151)

**Other countries**[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=57)]

* CERT [Brazil](https://en.wikipedia.org/wiki/Brazil), member of FIRST (Forum for Incident Response and Security Teams)
* CARNet CERT, [Croatia](https://en.wikipedia.org/wiki/Croatia), member of FIRST
* AE CERT, [United Arab Emirates](https://en.wikipedia.org/wiki/United_Arab_Emirates)
* SingCERT, [Singapore](https://en.wikipedia.org/wiki/Singapore)
* CERT-LEXSI, [France](https://en.wikipedia.org/wiki/France), [Canada](https://en.wikipedia.org/wiki/Canada), [Singapore](https://en.wikipedia.org/wiki/Singapore)
* INCIBE, [Spain](https://en.wikipedia.org/wiki/Spain)
* ID-CERT, [Indonesia](https://en.wikipedia.org/wiki/Indonesia)

Modern warfare[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=58)]

*Main article:*[*Cyberwarfare*](https://en.wikipedia.org/wiki/Cyberwarfare)

Cybersecurity is becoming increasingly important as more information and technology is being made available on cyberspace. There is growing concern among governments that cyberspace will become the next theatre of warfare. As Mark Clayton from the [*Christian Science Monitor*](https://en.wikipedia.org/wiki/Christian_Science_Monitor) described in an article titled "The New Cyber Arms Race":

In the future, wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships.[[152]](https://en.wikipedia.org/wiki/Computer_security#cite_note-The_new_cyber_arms_race-152)

This has led to new terms such as [*cyberwarfare*](https://en.wikipedia.org/wiki/Cyberwarfare) and [*cyberterrorism*](https://en.wikipedia.org/wiki/Cyberterrorism). More and more critical infrastructure is being controlled via computer programs that, while increasing efficiency, exposes new vulnerabilities. The test will be to see if governments and corporations that control critical systems such as energy, communications and other information will be able to prevent attacks before they occur. As Jay Cross, the chief scientist of the Internet Time Group, remarked, "Connectedness begets vulnerability."[[152]](https://en.wikipedia.org/wiki/Computer_security#cite_note-The_new_cyber_arms_race-152)

Job market[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=59)]

Cybersecurity is a fast-growing[[153]](https://en.wikipedia.org/wiki/Computer_security#cite_note-153) field of [IT](https://en.wikipedia.org/wiki/Information_technology) concerned with reducing organizations' risk of hack or data breach. According to research from the Enterprise Strategy Group, 46% of organizations say that they have a "problematic shortage" of cybersecurity skills in 2016, up from 28% in 2015.[[154]](https://en.wikipedia.org/wiki/Computer_security#cite_note-154) Commercial, government and non-governmental organizations all employ cybersecurity professionals. The fastest increases in demand for cybersecurity workers are in industries managing increasing volumes of consumer data such as finance, health care, and retail.[[155]](https://en.wikipedia.org/wiki/Computer_security#cite_note-155) However, the use of the term "cybersecurity" is more prevalent in government job descriptions.[[156]](https://en.wikipedia.org/wiki/Computer_security#cite_note-156)

Typical cybersecurity job titles and descriptions include:[[157]](https://en.wikipedia.org/wiki/Computer_security#cite_note-157)

**Security analyst**

Analyzes and assesses vulnerabilities in the infrastructure (software, hardware, networks), investigates using available tools and countermeasures to remedy the detected vulnerabilities, and recommends solutions and best practices. Analyzes and assesses damage to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. Tests for compliance with security policies and procedures. May assist in the creation, implementation, and/or management of security solutions.

**Security engineer**

Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and mounts incident response. Investigates and utilizes new technologies and processes to enhance security capabilities and implement improvements. May also review code or perform other [security engineering](https://en.wikipedia.org/wiki/Security_engineering) methodologies.

**Security architect**

Designs a security system or major components of a security system, and may head a security design team building a new security system.

**Security administrator**

Installs and manages organization-wide security systems. May also take on some of the tasks of a security analyst in smaller organizations.

**Chief Information Security Officer (CISO)**

A high-level management position responsible for the entire information security division/staff. The position may include hands-on technical work.

**Chief Security Officer (CSO)**

A high-level management position responsible for the entire security division/staff. A newer position now deemed needed as security risks grow.

**Security Consultant/Specialist/Intelligence**

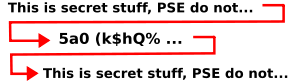
Broad titles that encompass any one or all of the other roles/titles, tasked with protecting computers, networks, software, data, and/or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, denial-of-service attacks, and an ever increasing list of attacks by hackers acting as individuals or as part of organized crime or foreign governments.

Student programs are also available to people interested in beginning a career in cybersecurity.[[158]](https://en.wikipedia.org/wiki/Computer_security#cite_note-158)[[159]](https://en.wikipedia.org/wiki/Computer_security#cite_note-159) Meanwhile, a flexible and effective option for [information security](https://en.wikipedia.org/wiki/Information_security)professionals of all experience levels to keep studying is online security training, including webcasts.[[160]](https://en.wikipedia.org/wiki/Computer_security#cite_note-160)[[161]](https://en.wikipedia.org/wiki/Computer_security#cite_note-161)[[162]](https://en.wikipedia.org/wiki/Computer_security#cite_note-162)

Terminology[[edit](https://en.wikipedia.org/w/index.php?title=Computer_security&action=edit&section=60)]

The following terms used with regards to engineering secure systems are explained below.

* Access [authorization](https://en.wikipedia.org/wiki/Authorization) restricts access to a computer to group of users through the use of [authentication](https://en.wikipedia.org/wiki/Authentication) systems. These systems can protect either the whole computer – such as through an interactive [login](https://en.wikipedia.org/wiki/Login) screen – or individual services, such as an [FTP](https://en.wikipedia.org/wiki/File_Transfer_Protocol) server. There are many methods for identifying and authenticating users, such as [passwords](https://en.wikipedia.org/wiki/Password), [identification cards](https://en.wikipedia.org/wiki/Identification_card), and, more recently, [smart cards](https://en.wikipedia.org/wiki/Smart_card) and [biometric](https://en.wikipedia.org/wiki/Biometric) systems.
* [Anti-virus software](https://en.wikipedia.org/wiki/Anti-virus_software) consists of computer programs that attempt to identify, thwart and eliminate [computer viruses](https://en.wikipedia.org/wiki/Computer_viruses) and other malicious software ([malware](https://en.wikipedia.org/wiki/Malware)).
* [Applications](https://en.wikipedia.org/wiki/Application_software) with known security flaws should not be run. Either leave it turned off until it can be patched or otherwise fixed, or delete it and replace it with some other application. Publicly known flaws are the main entry used by [worms](https://en.wikipedia.org/wiki/Computer_worm) to automatically break into a system and then spread to other systems connected to it. The security website [Secunia](https://en.wikipedia.org/wiki/Secunia) provides a search tool for unpatched known flaws in popular products.
* [Authentication](https://en.wikipedia.org/wiki/Authentication) techniques can be used to ensure that communication end-points are who they say they are.
* [Automated theorem proving](https://en.wikipedia.org/wiki/Automated_theorem_proving) and other verification tools can enable critical algorithms and code used in secure systems to be mathematically proven to meet their specifications.
* [Backups](https://en.wikipedia.org/wiki/Backup) are a way of securing information; they are another copy of all the important computer files kept in another location. These files are kept on hard disks, [CD-Rs](https://en.wikipedia.org/wiki/CD-R), [CD-RWs](https://en.wikipedia.org/wiki/CD-RW), [tapes](https://en.wikipedia.org/wiki/Magnetic_tape_data_storage) and more recently on the cloud. Suggested locations for backups are a fireproof, waterproof, and heat proof safe, or in a separate, offsite location than that in which the original files are contained. Some individuals and companies also keep their backups in [safe deposit boxes](https://en.wikipedia.org/wiki/Safe_deposit_box) inside [bank vaults](https://en.wikipedia.org/wiki/Bank_vault). There is also a fourth option, which involves using one of the [file hosting services](https://en.wikipedia.org/wiki/File_hosting_service) that backs up files over the [Internet](https://en.wikipedia.org/wiki/Internet) for both business and individuals, known as the cloud.
  + Backups are also important for reasons other than security. Natural disasters, such as earthquakes, hurricanes, or tornadoes, may strike the building where the computer is located. The building can be on fire, or an explosion may occur. There needs to be a recent backup at an alternate secure location, in case of such kind of disaster. Further, it is recommended that the alternate location be placed where the same disaster would not affect both locations. Examples of alternate disaster recovery sites being compromised by the same disaster that affected the primary site include having had a primary site in [World Trade Center](https://en.wikipedia.org/wiki/World_Trade_Center_(1973%E2%80%932001)) I and the recovery site in [7 World Trade Center](https://en.wikipedia.org/wiki/7_World_Trade_Center), both of which were destroyed in the [9/11](https://en.wikipedia.org/wiki/9/11) attack, and having one's primary site and recovery site in the same coastal region, which leads to both being vulnerable to hurricane damage (for example, primary site in New Orleans and recovery site in [Jefferson Parish](https://en.wikipedia.org/wiki/Jefferson_Parish), both of which were hit by [Hurricane Katrina](https://en.wikipedia.org/wiki/Hurricane_Katrina) in 2005). The backup media should be moved between the geographic sites in a secure manner, in order to prevent them from being stolen.
* [Capability](https://en.wikipedia.org/wiki/Capability_(computers)) and [access control list](https://en.wikipedia.org/wiki/Access_control_list) techniques can be used to ensure privilege separation and mandatory access control. [This section](https://en.wikipedia.org/wiki/Computer_security#Capabilities_vs._ACLs) discusses their use.
* [Chain of trust](https://en.wikipedia.org/wiki/Chain_of_trust) techniques can be used to attempt to ensure that all software loaded has been certified as authentic by the system's designers.
* [Confidentiality](https://en.wikipedia.org/wiki/Confidentiality) is the nondisclosure of information except to another authorized person.[[163]](https://en.wikipedia.org/wiki/Computer_security#cite_note-163)
* [Cryptographic](https://en.wikipedia.org/wiki/Cryptography) techniques can be used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified.
* [Cyberwarfare](https://en.wikipedia.org/wiki/Cyberwarfare) is an internet-based conflict that involves politically motivated attacks on information and information systems. Such attacks can, for example, disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems.
* [Data integrity](https://en.wikipedia.org/wiki/Data_integrity) is the accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record.[[164]](https://en.wikipedia.org/wiki/Computer_security#cite_note-164)

[](https://en.wikipedia.org/wiki/File:Encryption_-_decryption.svg)

[Cryptographic](https://en.wikipedia.org/wiki/Cryptography) techniques involve transforming information, scrambling it so it becomes unreadable during transmission. The intended recipient can unscramble the message; ideally, eavesdroppers cannot.

* [Encryption](https://en.wikipedia.org/wiki/Encryption) is used to protect the message from the eyes of others. [Cryptographically](https://en.wikipedia.org/wiki/Cryptography) secure [ciphers](https://en.wikipedia.org/wiki/Cipher) are designed to make any practical attempt of [breaking](https://en.wikipedia.org/wiki/Cryptanalysis) infeasible. [Symmetric-key](https://en.wikipedia.org/wiki/Symmetric-key_algorithm) ciphers are suitable for bulk encryption using [shared keys](https://en.wikipedia.org/wiki/Shared_key), and [public-key encryption](https://en.wikipedia.org/wiki/Public-key_encryption) using [digital certificates](https://en.wikipedia.org/wiki/Digital_certificate) can provide a practical solution for the problem of securely communicating when no key is shared in advance.
* [Endpoint security](https://en.wikipedia.org/wiki/Endpoint_security) software helps networks to prevent exfiltration (data theft) and virus infection at network entry points made vulnerable by the prevalence of potentially infected portable computing devices, such as laptops and mobile devices, and external storage devices, such as USB drives.[[165]](https://en.wikipedia.org/wiki/Computer_security#cite_note-165)
* [Firewalls](https://en.wikipedia.org/wiki/Firewall_(networking)) are an important method for control and security on the Internet and other networks. A network firewall can be a communications processor, typically a router, or a dedicated server, along with firewall software. A firewall serves as a gatekeeper system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks. It screens all network traffic for proper passwords or other security codes and only allows authorized transmission in and out of the network. Firewalls can deter, but not completely prevent, unauthorized access (hacking) into computer networks; they can also provide some protection from online intrusion.
* [Honey pots](https://en.wikipedia.org/wiki/Honeypot_(computing)) are computers that are either intentionally or unintentionally left vulnerable to attack by crackers. They can be used to catch crackers or fix vulnerabilities.
* [Intrusion-detection systems](https://en.wikipedia.org/wiki/Intrusion-detection_system) can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.
* A [microkernel](https://en.wikipedia.org/wiki/Microkernel) is the near-minimum amount of software that can provide the mechanisms to implement an operating system. It is used solely to provide very low-level, very precisely defined machine code upon which an operating system can be developed. A simple example is the early '90s GEMSOS (Gemini Computers), which provided extremely low-level machine code, such as "segment" management, atop which an operating system could be built. The theory (in the case of "segments") was that—rather than have the operating system itself worry about mandatory access separation by means of military-style labeling—it is safer if a low-level, independently scrutinized module can be charged **solely** with the management of individually labeled segments, be they memory "segments" or file system "segments" or executable text "segments." If software below the visibility of the operating system is (as in this case) charged with labeling, there is no theoretically viable means for a clever hacker to subvert the labeling scheme, since the operating system *per se* does **not** provide mechanisms for interfering with labeling: the operating system is, essentially, a client (an "application," arguably) atop the microkernel and, as such, subject to its restrictions.
* [Pinging](https://en.wikipedia.org/wiki/Ping_(networking_utility)) The ping application can be used by potential crackers to find if an IP address is reachable. If a cracker finds a computer, they can try a port scan to detect and attack services on that computer.
* [Social engineering](https://en.wikipedia.org/wiki/Social_engineering_(computer_security)) awareness keeps employees aware of the dangers of social engineering and/or having a policy in place to prevent social engineering can reduce successful breaches of the network and servers.