**Biometrics** is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication)[[note 1]](https://en.wikipedia.org/wiki/Biometrics#cite_note-1) is used in computer science as a form of identification and [access control](https://en.wikipedia.org/wiki/Access_control).[[1]](https://en.wikipedia.org/wiki/Biometrics#cite_note-2)[[2]](https://en.wikipedia.org/wiki/Biometrics#cite_note-3) It is also used to identify individuals in groups that are under [surveillance](https://en.wikipedia.org/wiki/Surveillance).

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals.[[3]](https://en.wikipedia.org/wiki/Biometrics#cite_note-JainA-4) Biometric identifiers are often categorized as physiological versus behavioural characteristics.[[4]](https://en.wikipedia.org/wiki/Biometrics#cite_note-Jain1-5) Physiological characteristics are related to the shape of the body. Examples include, but are not limited to [fingerprint](https://en.wikipedia.org/wiki/Fingerprint), palm veins, [face recognition](https://en.wikipedia.org/wiki/Facial_recognition_system), [DNA](https://en.wikipedia.org/wiki/DNA), [palm print](https://en.wikipedia.org/wiki/Palm_print), [hand geometry](https://en.wikipedia.org/wiki/Hand_geometry), [iris recognition](https://en.wikipedia.org/wiki/Iris_recognition), [retina](https://en.wikipedia.org/wiki/Retinal_scan) and odour/scent. Behavioural characteristics are related to the pattern of behaviour of a person, including but not limited to [typing rhythm](https://en.wikipedia.org/wiki/Keystroke_dynamics), [gait](https://en.wikipedia.org/wiki/Gait_analysis), and [voice](https://en.wikipedia.org/wiki/Speaker_recognition).[[5]](https://en.wikipedia.org/wiki/Biometrics#cite_note-6)[[note 2]](https://en.wikipedia.org/wiki/Biometrics#cite_note-7) Some researchers have coined the term betamimetics to describe the latter class of biometrics.[[6]](https://en.wikipedia.org/wiki/Biometrics#cite_note-8)

More traditional means of access control include token-based identification systems, such as a [driver's license](https://en.wikipedia.org/wiki/Driver%27s_license) or [passport](https://en.wikipedia.org/wiki/Passport), and knowledge-based identification systems, such as a [password](https://en.wikipedia.org/wiki/Password) or [personal identification number](https://en.wikipedia.org/wiki/Personal_identification_number).[[3]](https://en.wikipedia.org/wiki/Biometrics#cite_note-JainA-4) Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises [privacy concerns](https://en.wikipedia.org/wiki/Biometrics#Privacy_and_discrimination) about the ultimate use of this information.[[3]](https://en.wikipedia.org/wiki/Biometrics#cite_note-JainA-4)[[7]](https://en.wikipedia.org/wiki/Biometrics#cite_note-Weaver-9)[[8]](https://en.wikipedia.org/wiki/Biometrics#cite_note-10)

Multimodal biometric systems use multiple sensors or biometrics to overcome the limitations of unimodal biometric systems.[[12]](https://en.wikipedia.org/wiki/Biometrics#cite_note-dca-15) For instance iris recognition systems can be compromised by aging irises[[13]](https://en.wikipedia.org/wiki/Biometrics#cite_note-16) and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken passcode).[[14]](https://en.wikipedia.org/wiki/Biometrics#cite_note-17)[[15]](https://en.wikipedia.org/wiki/Biometrics#cite_note-18)