Biometric devices grant access to programs, mobile devices, computers, or rooms using computer analysis of some personal characteristic. For example, types of biometric devices and systems consist of fingerprint readers, face recognition systems, hand geometry systems, voice verification systems, signature verification systems, and iris recognition systems or retinal scanners.

## Fingerprint Reader

A fingerprint reader, also called a fingerprint scanner, captures the curves and indentations of one’s fingerprint. Organizations use fingerprint readers to secure doors, computers, and software. With the cost of fingerprint readers often less than $100, some home and small business users purchase fingerprint readers to verify the identity of users before they can access a computer. The reader also can be set up to perform different functions for different fingers; for example, one finger runs a program and a different finger shuts down the computer. External fingerprint readers usually plug into a USB port.

Mobile computers, smartphones, and smartwatches often have a built-in fingerprint reader. Using their fingerprint, users can unlock the computer or device, sign in to programs and websites via their fingerprint instead of entering a user name and password, and on some devices, even test their blood pressure and heart rate.

## Face Recognition System

To determine whether a person is a legitimate user, a face recognition system captures their live face image and compares it with a stored image. Some buildings use face recognition systems to secure access to rooms. Law enforcement, surveillance systems, and airports often use face recognition to protect the public. Some mobile devices use face recognition systems to unlock the device. Face recognition programs are becoming more sophisticated and can recognize people with or without their glasses, makeup, or jewelry, and with new hairstyles.

## Hand Geometry System

Hand geometry systems measure the shape and size of a person’s hand. Because these systems can be expensive, they often are used in larger companies to track workers’ time and attendance or as security devices. Colleges use hand geometry systems to verify students’ identities. Daycare centers and hospital nurseries use them to identify parents who pick up their children.

## Voice Verification System

A voice verification system will compare a person’s live speech with their stored voice pattern. Larger organizations sometimes use voice verification systems as time and attendance devices. Many companies also use this technology for access to sensitive files and networks. To secure phone banking transactions, some financial services use voice verification systems.

## Signature Verification System

A signature verification system recognizes the shape of your handwritten signature, as well as measures the pressure exerted and the motion used to write the signature. Signature verification systems use a specialized pen and tablet. Signature verification systems often are used to reduce fraud in financial institutions.

## Iris Recognition System

High security areas often use iris recognition systems. The camera in an iris recognition system uses iris recognition technology to read patterns in the iris of the eye. These patterns are as unique as a fingerprint. Iris recognition systems are quite expensive and are used by financial institutions that deal with highly sensitive data, government security organizations, and the military. Some organizations use retinal scanners, which work similarly but instead scan patterns of blood vessels in the back of the retina.

## Biometric Devices

Biometric devices are gaining popularity as a security precaution because they are a virtually foolproof method to verify an identity. For example, some grocery stores, retail stores, and gas stations use biometric payment, where the customer’s fingerprint is read by a fingerprint reader that is linked to a payment method, such as a checking account or credit card.

Users can forget their user names and passwords. Badges, identification cards, and keys can be lost, copied, duplicated, or stolen. Personal characteristics, by contrast, are unique and cannot be forgotten or misplaced.

Biometric devices, however, do have some disadvantages. If you cut your finger, a fingerprint reader might reject you as a legitimate user. Hand geometry readers can transmit germs. If you are nervous, a signature might not match the one on file. If you have a sore throat, a voice recognition system might reject you. Many people are uncomfortable with using an iris or retinal scanner.