Biometrics is a unique and effective security technology that authenticates a person’s identity by verifying personal characteristics. Biometric devices grant users access to programs, systems, or rooms by analyzing some biometric identifier, such as a fingerprint or eye pattern. Two commonly used types of biometric security devices are fingerprint readers and iris recognition systems.

A fingerprint reader captures the curves and indentations of a fingerprint. Fingerprint readers can be set up to perform different functions for different fingers. For example, the index finger could start a program, and the ring finger could shut down the computer (Jenkins). Fingerprint readers usually cost less than $100, making it easy for people to use them in personal and business environments. Newer computer models include internal fingerprint readers for added security. External fingerprint readers usually are connected to a USB port on the computer (Parlor).

A biometric security device used in high security areas is an iris recognition system. Iris recognition systems 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 government security organizations, the military, and financial institutions that deal with highly sensitive data (Doe)[[1]](#footnote-1).

Biometric technology is a very effective way to keep information secure. Biometric technology is used in several different ways. Two widely known biometric devices are fingerprint readers and iris recognition systems. With biometric technology, the world can be more secure.

Works Cited

1. Some organizations use retinal scanners, which work similarly but instead scan patterns of blood vessels in the back of the retina. [↑](#footnote-ref-1)