Security is one of the major issues today in a society that is technologically connected. Mobile devices are now not only used for making and receiving calls, but also for transferring money, paying bills, or sharing health records. When this becomes an everyday routine, users do not want to spend too much time thinking about their device security. They expect that security should be a seamless part of the device or technology they use. Hence, all major mobile device manufacturers have started to integrate security features, like two-factor authentication or biometric authentication. The use of fingerprint authentication is common among biometrics. However, mobile manufacturers are now also using iris scanning technology to ensure optimum security of devices. This takes security to another level, and generally makes it very hard for cyber criminals to steal a user’s identity along with their financial or personal information.

## Why Do We Need Tougher Protection?

Though password remains to be the most widely used form of protecting identity, it can be exploited if a user is negligent. Individuals often keep poor security practices such as choosing weak passwords, reusing passwords, and even sharing them with people they trust. It is also not uncommon for users to share passwords over calls, email or messages, which increases their risks of compromised security. Passwords can also be compromised by phishing practices such as fraudulent emails or phone calls. It also increases risks of identity theft, particularly when financial information is [transmitted](http://www.cardzgroup.com/ContactSmartCard.html) online over unsecured networks. This is why, an additional layer of security is required which makes it harder for criminals to get through your system.

## Biometrics Brings New Functionality

Biometrics security has been a part of mobile industry since 2011, when mobile device manufacturers started using fingerprint technology. At that time, it was used for unlocking devices. Now, it is being seamlessly integrated into mobile services and applications, particularly payment applications. This is because the benefits and functionality it provides to users alongside security is critical to its increased acceptance.

## Iris Scanning Improves Ease of Use and Enhances Security

As with other biometrics, iris scanning is continuing to gain popularity. Initially, using human eyes to access devices and unlock doors was only seen in movies, but now it is a widely-accepted reality. The human iris is also protected by cornea, so it does not change much as people grow older. It brings increased security to consumers due to its complexity, which makes it almost impossible to be replicated. Fingerprint scanning only recognizes 40 unique individual traits, whereas iris scanning recognizes 266, making it more secure than fingerprint authentication – which is most widely-used form of biometric authentication at present.

Furthermore, since iris scanning only needs a user to look at a device, it is also fairly user friendly and simple to use. Also worth mentioning is the ability it provides the user to authenticate themselves without touching anything – making it ideal for social distancing. Where iris scanning improves device security, it also decreases the time spent in unlocking devices, thus improving usability and eliminating the need to use passwords.

## Iris Scanning Challenges

Although iris scanning provides greater security and usability, it still comes with challenges. Firstly, for people to use it, it must work as quickly and accurately as fingerprint technology – or even better. If biometric authentication is not fast and effortless, users may not prefer to use it.

Moreover, it must be able to work along with other biometric authentication technologies for improved security. For people to trust iris scanning, biometric data must be stored as securely as other biometric technologies and verified likewise.

Iris scanning also suffers from the same issues as other biometric authentication methods in that they depend upon operating systems and application developers for enabling biometric authentication besides only unlocking a device.

## Final Thoughts

Iris recognition technology has applications in a wide range of areas, including physical access control, national citizen identity programs, and border management. It can also be used to authenticate users on mobile devices that have IR-enabled cameras. With its advantages over voice, fingerprints, face, and other biometrics, iris scanning will prove as a better authentication method over time. It will provide a more reliable and safer solution to one of the biggest pain points in modern-day technology – the use of passwords. Hence, iris recognition is undoubtedly the next step in the evolution of smartphone security.