Membership Magazine July, 2024

SMART GUNS AND BIOMETRIC TECHNOLOGY

682-238-8161 I Email: sdfmembers@gmail.com I www.selfdefensefund.net

WHAT IS BIOMETRIC AUTHENTICATION, AND HOW SECURE IS IT?

Many of us use biometric identification to unlock our PC's, Macs, Androids, iPhones, and other devices. First, we set up biometric authentication when we purchase a new device, which stores biometric data about our specific characteristics in "The Cloud." Then, anytime we try to unlock the device, it references the stored biometric data in The Cloud. Smart guns, also known as "personalized firearms," also use this technology.

SMART GUNS HAVE BEEN FOR SALE FOR OVER TEN YEARS BUT THE QUESTION IS DOES ANYONE WANT IT?

The latest version was introduced by a company called BIOFIRE.

The term "The Cloud" is virtual and not physical. It is a group of computer servers running in a cloud computing environment that can be accessed on demand by unlimited users.

IS CLOUD STORAGE SAFE, SECURE, AND PRIVATE?

It depends on The Cloud storage provider's reputation and reviews and who owns it! This may sound a little obvious, but checking out reviews of a cloud storage provider can help you narrow down which cloud is the most secure and private. Most of the time, how safe a cloud is boils down to technical things that can be hard to comprehend unless you have a degree in computer science or engineering.

Chances are you use biometrics every day to unlock your devices without giving the process much thought. The technology is the latest advancement in security and the protection of devices against unwanted intrusion. Many of us know very little about how biometrics work and how secure our biometric data really is.

BIOMETRIC SECURITY CONCERNS
HOW SAFE IS YOUR DATA?

Biometrics does offer better security than usernames and passwords, but nothing in this world is 100% safe and secure. If stolen, your biometric data could be used to access your entire digital life.

SOME OF THE COMMON CONCERNS ABOUT BIOMETRIC SAFETY INCLUDE

- ***Hacking***

  Although it takes a sophisticated hacker to use them, your biometrics are an attractive target. The more places you use biometrics, the more exposed you are to theft.

- ***Duplication***

  Unfortunately, some biometric data is easy to duplicate. Fingerprints, for example, can be lifted off a common drinking glass. Cybercriminals are quickly learning how to steal this data and use it for personal gain.

- ***Risk***

  Your biometric characteristics are etched in stone, and you cannot change them as easily as you can change a password, making it risky if they are stolen.

- ***Complacency***

  Users could be careless when using biometrics and expose themselves to bad actors.

- ***Privacy***

  Many devices, including smart home screens and other electronics, collect biometric data like your voice. It makes you wonder how private your details are and what companies are doing with all this data.

- ***Cloning***

  Hackers have found ways to duplicate fingerprints and even fool facial recognition scanners.

- ***Human error***

  This is another factor that makes biometrics vulnerable. People make mistakes. They rush things and don't always remember to follow cybersecurity best practices.

Although biometrics offers users a secure, convenient, and high-tech way to access devices and resources, this doesn't come without some risks. Be careful with whom you choose to share your biometrics.

While opting in for these features on a device like your phone is probably a good idea, be cautious when dealing with companies you aren't as familiar with. You never know how they are using your data or with whom they are sharing it. For added protection, always turn on two-factor authentication so that even if one authentication method is compromised, your data will remain protected by another layer of security.

This guide will explain what biometrics are, how they work to keep you safe and secure, the different types, and any security concerns you might have.