**CTF Challenge: Biometric Security and its Implications**

****

**Biometric Security?**

****

Biometric security involves using individuals' unique biological traits for identification and access control. Common biometric identifiers include fingerprints, facial recognition, iris patterns, voice recognition, and even behavioral patterns such as typing rhythm. While biometric security offers many advantages, it also poses significant challenges and implications.

### **Advantages of Biometric Security**

1. **Enhanced Security:**
   * Biometrics provide a higher level of security compared to traditional passwords or PINs because they are unique to each individual and difficult to replicate or steal.
2. **Convenience:**
   * Biometric authentication is quick and user-friendly, eliminating the need for remembering passwords or carrying tokens.
   * It streamlines processes in various applications, such as unlocking devices or accessing secure areas.
3. **Non-Repudiation:**
   * Biometric data uniquely identifies an individual, providing a high level of assurance in transactions and access controls.
   * Reduces the risk of impersonation and fraud.
4. **Efficiency:**
   * Biometric systems can process large numbers of individuals quickly, making them suitable for high-traffic environments like airports and secure facilities.

# **Capture the Flag (CTF) Challenges**

Flag 1. What does biometric security use for identification?

**Answer: Traits**

Flag 2. What biometric identifier involves analyzing eye patterns?

**Answer: Iris**

Flag 3. Which biometric feature can be affected by aging or injury?

**Answer: Fingerprint**

Flag 4. What concept ensures a person's identity in transactions and access controls?

**Answer: Non-Repudiation**

Flag 5. In which environment are biometric systems particularly efficient?

**Answer: Airports OR Secure facilities**