Authentication Write-Up

Throughout the years, technology has brough about revolutionary advancements, including the ability to personalize devices. People can now create profiles that store almost every detail of their lives ranging from contacts and photos to banking information. As a result, it became essential for tech companies to implement a verification process to confirm a users identity, known as authentication. Authentication systems act as barriers that prevent hackers from gaining access to private data. Unfortunately, many users underestimate the seriousness of identitfy theft. Cybercriminals can steal private information and impersonate individuals for fraudulent or criminal activites.

There are many simple ways a user can protect their data including passwords, pins, patterns, fingerprints, emails and phone numbers. The basic and widely used form of authentication is password. Devices usually request a username and complex password. Complexity plays a huge factor since it will make hacking more challenging for hackers. On the other hand, Biometrics operate by recognizing a unique physical characteristic of the user such as fingerprints. Modern devices often include multifactor authentication, combining two or more methods like fingerprints with passwords or email verification. These systems ensure that only the rightful user can access sensitive information.