Life Beyond Passwords: Biometrics and the Future of User Verification

Kingdoms once protected vast treasures of gold and jewels with secret vaults and well-armed guards. Now, computer networks and even mobile devices grant access to our most valuable assets. As cyber risks evolve, businesses and individuals must also evolve beyond passwords to more sophisticated authentication methods.

The obvious next step beyond passwords involves biometrics as part of a multi-factor authentication (MFA) process. For instance, anyone who purchased a new cellphone in the last couple of years has likely used facial recognition to access the phone and various apps.

Biometrics offers quick access with a relatively high degree of security. And with a variety of methods available, from facial recognition to fingerprints and eye scans, organizations have choices to make. Understanding the pros and cons of some of those options can help organizations navigate life beyond passwords.

Physical vs. Behavioral Biometrics

Biometrics can involve physiological or behavioral characteristics. For example, physiological biometrics include characteristics like fingerprints, face shape, vein patterns and the iris or retina. Most of these characteristics remain stable throughout life.

Behavioral biometrics, on the other hand, involve the way we do things. Examples include the way we talk, the way we type on a keyboard or how we walk. While useful, these characteristics can change with stress, disease or other life experiences making them less useful for authentication.

Common Types of Biometrics

As far back as the late 1800s, Mark Twain wrote about the use of fingerprints for identification. But Twain could not have imagined the progress biometrics would make over the next 150 years. Now, most of us encounter some form of biometrics nearly every day. Biometric technology has increased security while providing quick access to authorized users.

Consider the advantages and disadvantages of these common biometric methods:

- **Fingerprints** – After decades of development, fingerprint technology offers an accurate, familiar and relatively economical method of biometric authentication. However, scars or even sweat and dirt can alter the fingerprint and result in rejection of an authorized user.
- **Facial recognition** – Like fingerprints, facial recognition offers quick and easy authentication. However, while facial recognition technology has evolved significantly in recent years, the modality still has a low degree of accuracy as compared to other options.
- **Iris scans** – Iris scans offer the highest degree of accuracy, and the iris does not change over time. However, iris scanners require significant investment. And a hacker could potentially trick an iris scanner with a high-quality photograph.
- **Retina scans** – Retina scans also offer a high degree of accuracy. However, while hackers find retina scans more difficult to trick, the retina can change over time due to diseases such as diabetes or glaucoma.

- **Palm scans** – The vein pattern in the human palm is both unique to each individual and complex. Thus, a palm scan offers a highly accurate identification method that hackers find extremely difficult to replicate. In fact, Amazon just announced a plan to develop new point of sale technology that will use hand scanners.
- **Voice recognition** – Increasingly sophisticated voice recognition systems analyze not only the sound and shape of the voice but also breathing and speech patterns. However, hackers may be able to fool the system with a high-quality recording.

Biometrics Trends to Watch

In addition to continual improvements to standard biometrics like face and voice recognition, watch for newer developments, such as ear or heartbeat biometrics or brain wave pattern analysis. Some experts look to modalities such as these as the future of biometrics. Other methods, like odor or sweat recognition, sound odd but might hold promise, as well.

Perhaps more importantly, some organizations have begun to use multimodal biometric systems. These systems take MFA to a new level by utilizing at least two biometric methods to verify user identity.

Tap into the Possibilities Beyond Passwords

Organizations can no longer depend on password technology alone to secure vital information and processes. Fortunately, advances in biometrics have begun to make additional security layers more accessible. Contact eMazzanti Technologies today to begin building a multi-layer cyber security solution that incorporates biometrics.