Can You Prevent Hacking with Biometrics?

A data breach can be life threating. A facility breach, unauthorized access, can be internal or external. Surprisingly, not all data breaches are from hackers. Disgruntled employees are the cause of 25% of data breaches according to a 2017 Verizon report, an important statistic to consider.

Traditionally, digital security and physical security were two separate departments. Today, these departments are increasingly working together and looking at the same technology to prevent hacking/unauthorized access to their data and facilities: Biometrics.

FaceKey offers access control systems that use two biometric credentials, i.e. fingerprints and faces for identification.

Despite popular claims, many are concerned that cybercriminals will be able to hack their biometric credentials: the fingerprints and faces. **CAN THEY?**

Questions about biometric technology to consider:

- Storage of the biometric characteristics - FaceKey converts the fingerprints and faces into a numerical code and also encrypts transmission of data between devices/readers. Not even FaceKey can convert that code back to a face or fingerprint.

- Is your fingerprint really unique when used as a credential – FaceKey uses pattern recognition to ensure that the fingerprint or even face credential is unique. If the biometric technology used is minutiae point analysis, the fingerprint might not be unique.

- Features of a robust biometric security solution – FaceKey believes that because all their credentials and transmissions of data are encrypted, the potential for hacking is zero.

- Why is biometrics your best defense for hackers and prevention of unauthorized access to your facilities? Everything in the FaceKey system that can be encrypted is encrypted. And, the false positive rate of recognition nears zero.

FaceKey offers access control systems that use two biometric credentials, i.e. fingerprints and faces for identification. With the FaceKey systems, only authorized employees can access facilities and sensitive areas such as document storage and server rooms and an electronic record is always made when an area is accessed. In addition, the systems make it easy to change areas or doors or cabinets an employee is allowed to access or to quickly delete an employee across the entire system.

For many organizations, the likelihood of a data breach from an outsider or an employee can be significantly reduced with the adoption of a biometric based access control system when combined with a thoughtful plan of who and when can access key areas. FaceKey systems are suitable for new installs or replacement for card readers in existing systems. The systems run on the network and are competitively priced.

FaceKey's opinion: FaceKey understands that it is impossible to build a product or system that cannot ever be hacked. However: we believe that to hack the FaceKey products will require the highest level of skill, money and time, neither of which is in abundant supply.

Give me a call to discuss your options. Call 210-826-8811 or email at sales@facekey.com. For more details visit http://www.facekey.com.

Contact:

Annette Starkweather
President
sales@facekey.com
210-826-8811