Biometric Signature ID

Reinvented Password Eliminates Fraud

Passwords. Most people would say they hate passwords and for good reason. They are growing increasingly more complicated; upper, lower, special characters and insanely long, not to mention the dreaded reset. From a security standpoint, passwords are hacked and compromised in multiple ways exposing systems and data to hackers. Biometric Signature ID (BSI) has created the first-of-its-kind technology which requires users to draw their passwords instead of typing them. BSI's product BioSig-ID™ authenticates user identities by the way they draw their passwords. During password enrollment, it records the pattern created by capturing the length, speed, direction, angle and more metrics of how it is drawn. "BioSig-ID turns the pattern into a highly secure biometric password that even if discovered, cannot be replicated by anyone other than the owner because of their unique pattern of biometrics. A 4 character biometric password turns itself into a multi-factor authentication methodology," says Jeff Maynard CEO and Founder. "It combines unique biometric gestures with password knowledge which removes the need for hardware that is usually required for biometrics."

Jeff Maynard

> Institutions use our technology to prevent data breaches and financial fraud by stopping access to fraudsters by locking the doors

The technology takes a two-defense approach to security. The first is plugging areas of known access opportunities while the second is searching for new access opportunities that can be compromised. "Institutions use our technology to prevent data breaches and financial fraud by stopping access to fraudsters by locking the doors to your assets. The technology can easily be integrated using common security protocols and since it does not require hardware or software downloads users report a 98 percent positive user experience," says Maynard.

BioSig-ID is a multifactor authenticator in a single product and has been independently tested to be as accurate as a fingerprint without the need for special equipment. If ever hacked, and unlike physical biometrics, the BioSig-ID password can be reset with a simple re-enrollment. Physical biometrics such as fingerprints, palm scans, face recognition cannot be reset if the system is compromised. "You cannot grow new ones and you can't use them again to guard against imposters," quips Maynard.

BSI has created 4 products. BioTect-ID™, for example, utilizes the same technology to lock down devices, including desktops, laptops, tablets and mobile phones that operate in a Windows™ environment. This added security ensures the devices remain locked and secure unless authenticated through the unique biometric password. Sharing of passwords goes away.

High-risk transactions like bill payments or wire transfers can also be secured with BSI's biometric technologies. For example, companies may make the user login to the app/portal using their simple pin or password, but to authorize a transaction, the user would be asked to provide the biometric signature first to verify their identity.

All BioSig-ID™ solutions include a fraud-detection reporting tool that makes use of HALT (History, Activity, Location, and Time) technology. Forensics looks at dozens of patterns to determine whether the person logging in is the registered account holder and if there are account access irregularities or impersonation activities.

Typical fraud discovered involved a person who created 12 fictitious accounts at a college attempting to commit financial aid fraud. Because the college utilized BioSig-ID™, the forensic reporting found the imposter used the same IP address, stroke count, and password to create 12 fictitious accounts. It is impossible to create 12 different gesture biometric signatures and remember the corresponding fictitious identity. The person was reported before any funds were dispersed and before any fraud could occur.

BSI is currently focused on accelerating their forensics activity with highly predictive and unique tools that identify real-time threats and better ways to prevent newer access opportunities. Additionally, BSI intends to branch into the consumer space by offering its services to secure personal devices and social media accounts from unwanted access. CT