BIOMETRIC PASSWORDS ARE NOW READY FOR PRIME TIME – READ THIS

A look at how BioSig-ID can save you time and money with a revolutionary new spin on unique biometric authentication

By: Jeff Maynard, President, Founder and CEO, Biometric Signature ID

Case Study

Identity fraud is mostly the result of data breaches. Data breaches are mostly the result of "INSANITY". That's right, INSANITY. One definition of INSANITY is to keep doing the same thing and hope something different will happen. Companies keep exposing valuable corporate assets using only a password as protection – that's INSANITY. Hackers have moved beyond passwords in their current form. Just ask all the companies who have paid an estimated $1B in restitution to their clients because of password stealing. (mostly). (Anthem to pay a record $115M to settle data breach suit) These companies would love the chance for a do over using something more secure to protect the family jewels.

What to use? The trick is to balance security against the user experience. What options are off the table?

Reliability kicks these options off:

- security questions (only 50% reliable (Read the latest on IRS hacking and the 50% failure of security questions)
- Texting a password to your phone (SMS is no longer secure)
- keystroke typing/biometrics (very low accuracy to name a few.)

End user experience. Physical biometrics (face, voice, iris, vein, fingerprint) are more accurate and great for physical access say buildings etc. but not ideal for remote/device logins. Thus, use as passwords is not recommended because they require extra hardware and cost more and it's just not practical to have/distribute a piece of hardware. Liability costs must be considered for physical biometrics since you can't replace if stolen or lost (can't grow new fingers). Privacy laws - the subject of class action lawsuits against companies Facebook, Google, Shutterfly etc. for collecting face images are also giving users cause for thought about using physical biometrics. (class action lawsuits against Shutterfly and Facebook)

Behavioral biometrics that look at continuous patterns of typing, swipe, and hold on your devices to enable users to authenticate themselves through their own behavior patterns are also being tested. However, the litmus test of catching bad actors is not conclusive as testing for false positives is difficult and the time it takes to build a pattern is too long to be useful. Some of the companies who offer this technology claim they capture many types of small patterns (accelerometer, gyroscope, pressure etc.) that can add up to something, but they also have to rely on biometrics such as keystroke which is not reliable nor accurate. Most of the patterns collected have also not been tested to find out if they really offer any value in identifying a user or fraudster. This is also mostly multi-layer not multi factor so a whole bunch of little patterns don't add up too much pattern depth and this will prevent uptake.

What are the other biometrics?

Gesture/Signature Based Biometrics offer a viable alternative. **Here's why** a product like BioSig-ID™ is ideally suited to be your secure password:

It is simple to use yet has proven reliability, high security and great user experience. Users DRAW/CREATE a password vs. typing one! Gesture biometrics of speed, direction, length,

height, width, angle are captured and stored. Only the “real” user can login and verify their identity. Impostors are stopped. Once successfully authenticated, users can access their virtual account, portable device, workstation or mobile app. BioSig-ID™ comes with an acute forensic activity audit trail report which has uncovered, identified and reduced online fraud.

Major benefits:

- Draw your password don’t type it
- No extra hardware is required, Users activate the software with their finger or mouse
- Third party tested at 99.97% accuracy (3x better than NIST guide)
- Use on all devices
- 98% positive user experience
- 11M uses in over 95 countries
- Stops password **sharing** the main cause of breaches

See BioSig-ID in action https://biosig-id.com/