Are passwords becoming a thing of the past?

Peter Harrison, Equifax Product Leader, Identity and Fraud, tells Perspective about the brave new world of biometric technology when it comes to identity authentication.

Passwords, ‘challenge questions’, number sequences, security tokens: these first-factor and second-factor secure authentication methods are not fool-proof. This is because they rely on something a person knows and that can be forgotten, or something that someone has and that can be lost or stolen.

The number of these we need to remember, or carry, in order to access our information, combined with the requirement to make them increasingly complex, means that our data may not be as secure as it needs to be.

Most people will end up using the same password to access numerous sites and the effort required to manage these, along with remembering tokens, can lead to user frustration and abandoned transactions.

Biometrics is being heralded as the answer, prompting people to ask whether the password is becoming a thing of the past.

Biometrics technologies measure and analyse human body characteristics for authentication purposes and can include DNA, fingerprints, eye retinas and rises, voice and face patterns, and hand measurements. While the use of biometrics is becoming increasingly common, there may still be some way to go before it becomes the default and singular option for secure and reliable ID authentication.

Biometric verification occurs when the biometric system attempts to confirm an individual’s claimed identity. It does this by comparing a submitted sample – such as their voiceprint – to one or more previously stored versions. It therefore works on what someone ‘is’ and can be a powerful tool for increasing security and avoiding fraud, especially when used in combination with other identity verification and authentication methods. It should therefore make it quicker and easier for the user to confirm their identity and gain access to the information, goods or services they want or need.

Time-honoured technology
Yet biometrics is not new: evidence suggests that fingerprints were used as a person’s mark as early as 500BC and early Chinese merchants used fingerprints to settle business transactions. Fingertips have also been used within law enforcement agencies for many years. While the principles remain the same, technology has developed at such a pace and proliferated into our everyday use to such an extent that it’s logical for it to impact on identity and security. The market is also significantly more valuable: Visiongain has put the value of the global biometrics market in 2012 at $7.59bn¹.

The use of biometric measures to authenticate customers is already out there, even though it’s not yet considered mainstream. Many of our clients are keen to explore the options and to understand the potential benefits. We are talking to them about how we are integrating biometrics into our product offerings, but as part of a layered and risk-based approach – to ensure the level of verification is appropriate to the value of the transaction – where there are always alternatives. We continue to work with organisations to discover what they are comfortable asking their customers to do in order to access their information or purchase goods. We are also sensitive to what customers are already using and what additional steps they will be prepared to take.

Biometric options
Face recognition is already used by many of us as a security measure on our mobile phones or tablets: “Face Unlock” is a feature that uses the unique features of a face to unlock Android smartphones.

There are also cases where face recognition is being used alongside, and to complement, a second factor, such as the electronic scanning of formal ID documents. This combination provides a two factor customer enrolment process, where something a person has, such as their passport, is copied and the content and photograph extracted, and something the person is, their face, is recorded. The checks also confirm that the document is not an obvious fake and, by automatically matching the recorded face to the photograph, the customer is confirmed as the owner of the passport.

An increasingly popular choice for many organisations is voice biometrics. This can be provided by creating a ‘voiceprint’ at the enrolment stage and can quickly and easily be captured with equipment that will exist in the majority of businesses, such as telephones, mobile phones, microphones and VOIP. But it is also robust and complex enough to ensure that it can’t easily be fooled, as it captures both physiological and behavioural traits within a person’s voiceprint.

Biometric signatures are also becoming more commonplace. PayPal has recently talked of its aim to move away from the password to embedded fingerprint scanners on mobile phones. Software that tracks the way a user moves their mouse, finger or stylus in order to create a password to log-in already exists.

The ethics of biometrics
So, while it is undoubtedly already combatting fraud and helping individuals and organisations protect data, the use of biometrics does continue to raise as many questions and challenges as it offers solutions. One of these is around privacy.

How will consumers feel about their biometric data being recorded and stored by organisations, even if that data is digitised? While a significant amount of data is already held, from personal to credit information, would biometrics be a step too far?

READ MORE
Are passwords becoming a thing of the past?

The pressure group, The Convention on Modern Liberty, has argued that the UK is already subject to an unnecessary accumulation of police powers. They state that “the collection of biometric data represents the top of a slippery slope that leads to the inevitable erosion of civil liberties and the beginnings of a surveillance state.”¹

The argument that the use of biometrics will be generally accepted is supported by the proliferation of data that people are already freely sharing with others – and not always with those they feel particularly close to. For example, many people are more than comfortable to allow tagged photos of them to be uploaded to Facebook on a regular basis. This not only provides consumers with a greater choice and assurance. It also affords them the convenience to quickly and easily access the products and services they want, without the associated hassle of remembering passwords. For both these reasons, it will, and should, be seen as a good thing.

A glitch in the matrix?

A final question has to be: will biometrics actually work? There needs to be consideration as to whether there will be too many false positives and/or false negatives.

Despite technological advances, environmental factors will undoubtedly affect outcomes; face recognition may be affected by lighting or the camera quality, and voice recognition by background noise or even whether the user has a cold. There may also be questions around accessibility; if someone’s speech is affected through disability and they’re unable to provide voice recognition, for example.

The element of convenience and ease of use in day-to-day situations must also be considered; an individual may be happy to share a login to an Apple iTunes account with a spouse where they use a common home computer; however, this is not an option if the login is protected by a fingerprint reader.

This leads me back to the premise raised at the start of this article: will biometrics mean that passwords become a thing of the past? Well, the answer is: probably not. At least for the time being, biometrics will need to be backed up by other factor authentication – either alongside or as a failsafe – which may mean remembering a password after all.

In addition, while biometrics like iris scanning might facilitate quick and easy recognition and login, initial enrolment into the system will still require an identity to be verified by non-biometric signifiers, such as a passport and/or by interactive ‘shared secret’ questions.

In fact, the ongoing use of biometric measures within account management should mean that the authentication of the customer at the point of enrolment is as strong as it can be to ensure that the biometric templates are attached to a genuine identity.

Going forward, biometrics will certainly provide another level of authentication for many organisations and, if used as part of a robust, consensual and multi-layered ID validation and authentication process, can be extremely effective in providing further security against fraud and moving us a step closer to a seamless or ‘friction-free’ user authentication model.

Equifax is in the process of introducing biometric measures into its growing array of identity and fraud services, where it will enable clients to apply biometric checks as part of a risk-based, progressive authentication approach. This means that checks are adapted to suit the transaction; high risk requires more robust measures, whereas low risk requires a light touch approach. The end result will mean more fraud is prevented, but also with an improved and more efficient customer experience.

For more information on our market leading identity verification and authentication solution, Equifax Identity Verifier, please contact Peter at peter.harrison@equifax.com or call 07887 596097.

² Biometrics: The Future at Our Finger Tips - Event Report by Dr Henry Kippin.