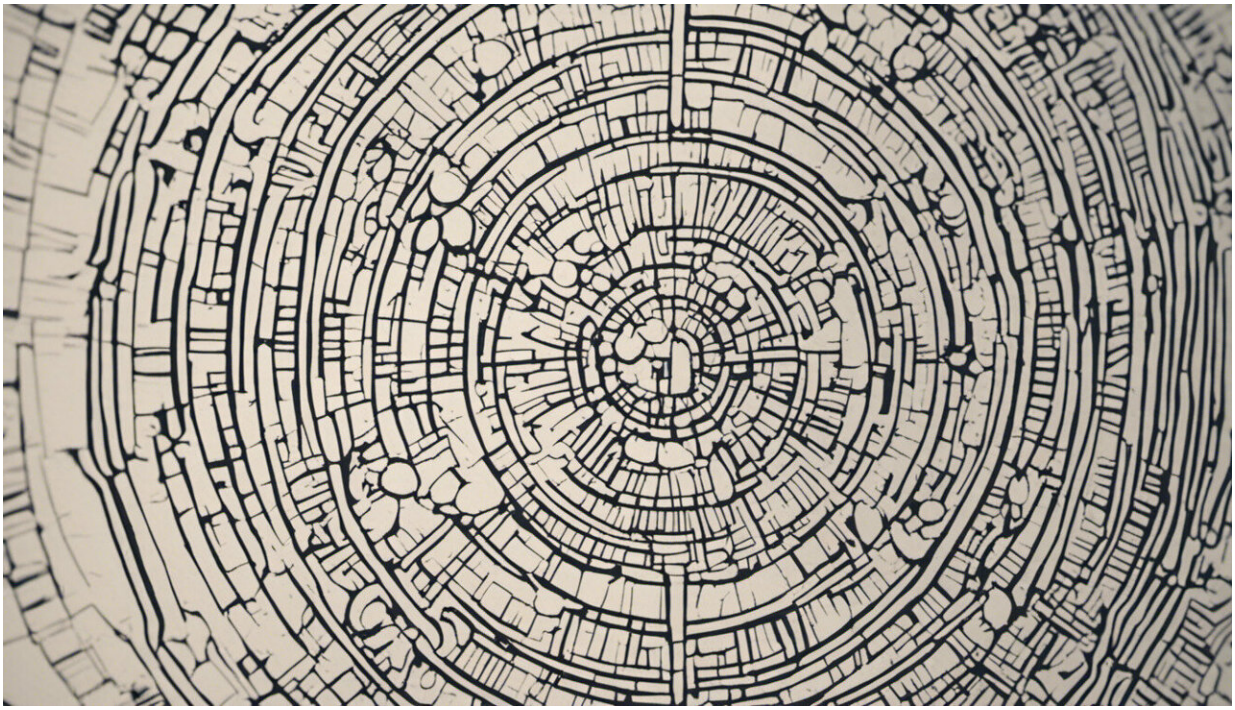
When your body becomes your password, the end of the login is nigh

March 23 2015, by Rob Miles



Credit: AI-generated image (disclaimer)

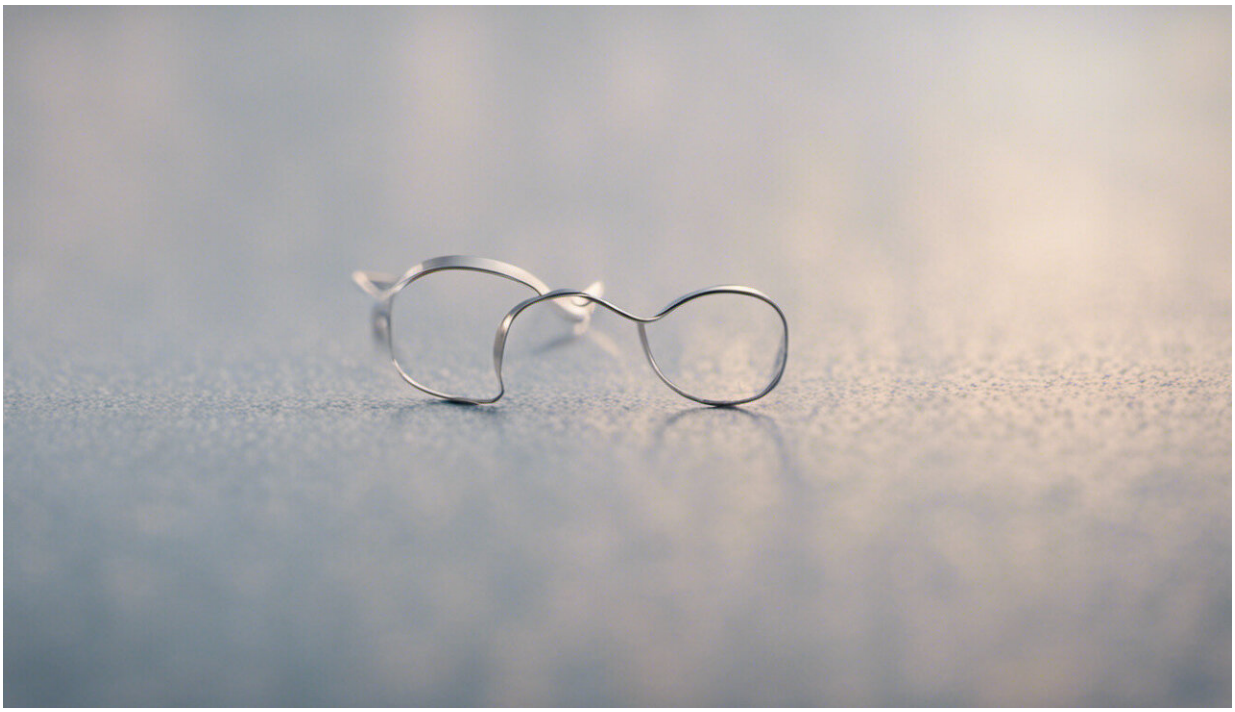
Passwords are a pain. I've just had to rummage around for the password required in order to post this article. I seem to have 100 or more different identities on different websites to manage. Whenever I book a flight or buy a concert ticket this often means setting up yet another persona and coming up with a password to authenticate it.

It's got so bad I've resorted to a password manager program to suggest secure, truly random passwords and then keep track of them for me. Of course if I forget the password to that program, or worse still if someone else guesses that password, I'll be in all sorts of trouble.

Your phone is the key

This is a recognised problem, so it's no surprise firms are looking at ways to make this easier. In the US, Yahoo has announced it plans to move to a password-on-demand system, where a new, one-time password is generated and texted to your mobile phone, and you can text the password to Yahoo's servers whenever its services require authentication.

This makes it things easier for the user, whose phone is now a key as well as everything else. But some security experts have been less than impressed. For example, many phones show the text of incoming messages automatically, popping up even when the phone is locked. All that would be required is five minutes alone with your phone and your Yahoo account could be hijacked. And who hasn't left their phone unattended for even just a short while?



Credit: AI-generated image (disclaimer)

How about your body?

All this hassle with usernames and passwords has led many to think biometrics are the answer, in which uniquely identifying elements of our physical body are used as authentication keys.

The most common, fingerprints, have been used as a means to authenticate users for some time. Fingerprint-based controlled access can be made to work reasonably well, although it is not immune to successful attack. When you find that Sherlock Holmes was cracking cases in 1903 which involved forged fingerprints, you might be forgiven for wondering if we really can provide security on the basis of our fingertips and thumbs. However, modern biometric security goes further to try to provide greater security.

Goodbye Windows password

Microsoft is building biometric password support into the forthcoming Windows 10, due to arrive later this year. The Windows Hello component, essentially a login screen, will be able to use a webcam to examine the user's face, iris, or a fingerprint scanner to unlock devices and provide Windows logon. Microsoft are also touting a mechanism built into its Passport service that will provide authentication on your behalf to other sites once you have successfully logged on to your computer and it has recognised you.

Halifax, the bank, has gone one step further for its online banking services. It is currently testing a smart wristband called Nymi which reads the wearer's heartbeat – another biometric measure that provides a rhythmic pattern that can be used as a unique identifier. Heartbeat biometrics are touted as harder to fake or fool than other biometrics, although when I consider what happens to my heartbeat when I check my bank balance I'd imagine it will need considerable testing.

Give me convenience or give me death

All this is a step toward the Holy Grail of authentication: security with convenience. Microsoft's moves in this direction are as part of the FIDO Alliance which aims to improve the way we approach security for devices and online services in the future, improving security and reducing the burden on users, which has a tendency to lead towards corner-cutting, weak or re-used passwords, and security compromises.

The good news for us password jugglers is that there is now a greater imperative behind building higher levels of security into systems from the outset, rather than trying to add it on afterwards, and that new and better ways of doing this are being expored. Modern devices, the latest

Dell tablet for example, have 3D cameras which can generate images that contain depth information as well as a visible picture. The wider introduction of these sorts of components and their successors will offer a way to provide a whole new way of authentication, to the point that in the not too distant future our smile really will be our passport.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation