

By continuing to use this site you consent to the use of cookies on your device as described in our [cookie policy](#) unless you have disabled them. You can change your [cookie settings](#) at any time but parts of our site will not function correctly without them.



Isn't it time your company's project management capability embraced the benefits of PRINCE2?



FINANCIAL TIMES

Home | World | Companies | Markets | Global Economy | Lex | Comment | Management | Life & Arts
 | Energy | | Financials | | Health | | Industrials | | Luxury 360 | | Media | | Retail & Consumer | | Tech | | Telecoms | | Transport | | By Region | | Tools |

September 26, 2014 5:07 pm

Tracks of our tears could hold key to cyber security

By Hannah Kuchler in San Francisco [Author alerts](#)



Tears can expose our most private emotions but could they also secure our most private information online?

Stephen Mason, an Australian optometrist, has discovered a new way to use scans of people's tears as passwords which he calls "the world's first one-time biometric pin".

He has focused on the cornea, rather than the iris, which is the norm in most optical scanners, because cyber criminals cannot copy the unique way tears change our eyes.

The scanner can recognise a person because each cornea has a unique map. But if a criminal was to steal and try to use the data from the last time someone logged in, the machine would find it invalid because it expects the data to change slightly each time.

"The corneal surface is wet with tears so our own data changes from moment to moment," he said. "Each data set I capture from any eye has these really tiny variations."

The hope is that the technology could be included on smartphones, from where it could be used to verify payments and access services such as email or sensitive corporate documents online. It could also be embedded in ATMs or doors to access confidential areas.

From intimate photos snatched and released online from celebrities' [Apple iCloud](#) accounts to an attack on [Home Depot](#), the largest known security breach of a retailer, the rise in cyber crime has experts searching for better ways to verify people's identities.

Simple passwords remain the most common way that individuals protect their data but many experts and technology companies believe this is an outdated form of protection and are turning to biometric alternatives.

Identity X, a US-based security company, uses voice identification as one factor for identifying people trying to access banking services remotely. Barclays Bank is set to launch scanners in the UK to identify some corporate customers using the unique vein patterns in their fingers.

Companies using more conventional fingerprint readers include Apple, which has one on its iPhone 5s and iPhone 6 devices, [Samsung](#), which includes one on the most recent Galaxy handset, and [Lenovo](#), the Chinese PC maker which has used them on its Thinkpad laptops.

Vinny Sakore, cloud security manager at the International Computer Security Association Labs, a security testing company, said passwords are probably the main reason why systems are breached.

One concern about existing biometric security systems is the risk of having the data stolen. Mr Mason said that people did not know what an exact copy of a fingerprint could be used for in the future.

But biometric technology is not the only potential solution. Many start-ups are trying to solve the same security problem, from password managers which store encrypted passwords and enter them on each site, to hardware key fobs which contain codes that are difficult to crack.

Mr Sakore cautioned that biometric technology "isn't quite there yet", with glitches such as not working with swollen fingers.

RELATED TOPICS [Cyber Security](#), [Apple Inc.](#), [Cyber Warfare](#)

Printed from: <http://www.ft.com/cms/s/0/b145bb98-404d-11e4-936b-00144feabdc0.html>

Print a single copy of this article for personal use. Contact us if you wish to print more to distribute to others.

© THE FINANCIAL TIMES LTD 2014 FT and 'Financial Times' are trademarks of The Financial Times Ltd.