Retinal scans and fingerprint checks: High tech or high risk?

April 22 2016, by Chris Marr, Sciencenetwork Wa

Credit: AI-generated image (disclaimer)

Having a smartphone unlock once it recognises your face or using a paypass machine that needs your fingerprint to finalise a purchase are becoming increasingly common, but are these the best way to stay secure?

Once consigned to spy movies like Mission Impossible: Rogue Nation biometric security features— such as fingerprint scans—are becoming part of everyday life but they are far from infallible, even without super spy Ethan Hunt to help you out.

Ways to authenticate people's identity come in three flavours—something you know, like a password, something you have, like a keycard, and something you are, like a fingerprint, which is considered biometrics.

The main issue with biometrics is the success rate ECU Security Research Institute expert Dr Clinton Carpene says.

"Biometric measures are prone to high rates of either false positives [where illegitimate users are allowed access to a system], or false negatives [where a legitimate user is denied access to a system they should be able to access]," Dr Carpene says.

Attempts to use biometrics to authenticate users and provide access to smartphones, for example, have proven unreliable at best, he says.

Facial recognition can be foiled by the simple use of a photograph, and voice recognition by the use of a recording.

Retinal scans have better potential, but who wants to have lasers shot into their eyes just to gain access to their smartphone?

Fingerprint recognition has already been introduced but our fingerprints can easily be "stolen"—we touch so many things every day that our fingerprints are everywhere and it isn't difficult to capture them.

Also a fingerprint can be damaged by wounds, chemicals or burning, or it could be covered in dirt and therefore unrecognisable.

"Given that biometrics are something that you are, they are something that can't be easily changed," he says.

For example, if a database of fingerprints needed to access a building was hacked, then that system is permanently compromised since the users cannot change their fingerprints.

But, a database of passwords that can be changed would not yield the same kind of vulnerability, he says.

Despite these potential shortcomings, biometrics are proving viable in commercial applications such as voice activating cars and smart TVs.

Biometric authentication mechanisms (fingerprint and/or facial recognition) are also becoming increasingly common for immigration purposes but these are further enhanced by human vigilance.

This article first appeared on ScienceNetwork Western Australia *a science news website based at Scitech.*

Provided by Science Network WA