

By [Sebastian](#) / [Internet / SEO News Editor](#)

[Blind Spot Eye Identification to Be Employed in Security Systems](#)

Japanese researchers hope

According to Japanese researchers working in the field of biometrics, the current security methods are far from being safe. And we're not talking here about easily hackable passwords, but iris or fingerprint identification. As specialists claim, with a little help from technology, people could easily imitate someone's features, even if this would imply drastic changes in a person's body, such as invasive surgery. Another obstacle could be that, say someone decides to go under the knife so that he/she could break into a particular account, he/she would first need to find out the details that need to be copied. "It is therefore desirable to devise biometric authentication that does not require biometric information to be kept secret," said the researchers, quoted by The Register. One of the methods that the Japanese specialists believe that should be employed in the future is identification based on the unique reflex response of the eyeball, which is different from the worn-out pupil dilatation when light hits the eye, because this one too has flaws, as the team claims. The reflex response scientists are referring to is related to the blind spot in every vertebrate eyeball. This is a minuscule spot that doesn't have any cone or rod cells, responsible with capturing light. In the futuristic biometric identification, a person's identity will be determined by measuring the time that sight needs in order to cover the distance between the blind spot and a previously fixed spot. "The expectation is that, even if a person's reflex characteristics are publicly known, it would be difficult for someone else to impersonate that person, since human beings are basically unable to control their own reflexes," added the researchers. An uncontrolled gesture would probably be the only method to stop identity thieves, although their fraud attempts will probably not stop. Scientists have not disclosed yet how much time would be necessary to actually implement the technology they believe is at least 99% safe.