

Putting a Face to a Secure Name



mobilesecurity.com [San Francisco, CA] Here at mobilesecurity.com we're not in the business of terrifying our visitors into submission. Take a look through the news sites out there, you'll find plenty of real-world examples that illustrate how important it is to invest in security software on any device that's connected to the internet. We're more about providing tips on how to prevent becoming a victim, and offering insight from experts working on the latest technology that's designed to keep your stuff protected. One simple way to keep your online accounts safe is to make sure you're using strong passwords.

Sure, there's keylogger technology that records every keystroke – and without sounding the alarm bells, you need to know that cybercriminals are increasingly determined to get their hands on your personal information. But with all the terrifying examples of why you should keep a close eye on your personal data, we wanted to let you know about a cool piece of new technology that's in development. What do you think of using facial recognition to increase the strength of password options (or just as a social media toy) – we think it sounds like a pretty good idea.... With reservations because it could also spell trouble for personal privacy or even make it easier for a thief to hack your phone.

The Shape of a Face

The way facial recognition software works is that it looks for symmetry (because most humans have symmetrical faces), and when it finds a shape it recognizes as a face, it measures the distance between specified markers (like the eyes and nose, for example), and then it uses an algorithm to match the control face to others like it.

Different brands of facial recognition software will use different features to recognize a person, which means that if you know what the software is measuring, you can fool it.

Fooling the Face

[Experiments](#) have found that while this technology is widely used by the military, law enforcement, security companies, and now Facebook and Google+, it is at best [92%](#) accurate. If the software version a company uses measures the distance between the eyes and nose, someone could go unrecognized if they simply cover the central part of their face. It was also found that by wearing big sunglasses (think *Breakfast at Tiffany's*) or asymmetrical costume makeup and artistic hairstyles, it may be possible to trick the system.

This is good news if facial recognition makes you nervous, bad news if you're a government agency trying to use it as a security tool. Regardless of whether or not the technology is 100% accurate, it represents an awesome power and could lead to scary infringements on personal privacy if not used responsibly. So how **is** it used?

Social Media and Security

[Facebook](#) uses facial recognition in order to spot you in photos that your friends post and then suggest to those friends that they tag you. Google+ and iPhoto do the same thing. This seems innocuous and if you've adjusted your security settings from the default option to more restrictive private options, it probably is. If the only people who can search for you or tag you in photos are your friends, or friends of friends, then facial recognition is probably more of a convenience than a caution.

But if your social media account is public, some security experts fear that eventually someone could take a photo of you at the grocery store, upload it to Facebook, and find out who you are. Now that new social media toy looks more like a tool for stalkers. But before you get up-in-arms, the study conducted by PC World found that the current technology isn't very good and only recognizes faces across multiple photos if the angles, lighting, coloring and facial expressions are similar.

If one of the variables is different, Facebook will probably still recognize you. But if in one photo you're smiling in great lighting and looking at the camera head on, and in another, you're looking to the left in a dimly-lit room, yelling at a television set, the computer will probably pass you by.

On the other hand, security companies, law enforcement officials and government agencies use facial recognition to promote safety. They scan crowds and security cameras to search out criminals and suspected terrorists and now Google and Microsoft have introduced the concept of facial recognition as an alternative to [passwords](#).

In theory, this is a great idea. The software either uses the image of your face as a way to unlock your phone, or you can set a photo from your computer as your password and then tap a specific area of the photo, or draw a line or circle to unlock your device.

[People](#) have expressed concern that the software is not foolproof and that by showing their

device a picture of themselves (as opposed to their actual face), they were able to unlock it. What security experts point out, is that facial recognition and picture passwords are not meant to be a foolproof, all-inclusive security measure. They are meant to give a more secure alternative to alphanumeric passwords that are easy to steal with the right spyware. They also protect your device should you leave it somewhere in a public place.

If you leave your phone on the bus, odds are, the person sitting next you doesn't know you, so they wouldn't be able to lock your phone using your photo. The software would therefore provide protection until you could recover your device or remotely wipe it.

Recommendations

Whether or not you are on the facial recognition bandwagon, its technology is on the rise and getting more proficient, so it's worth paying attention to. When it comes to social media, we always advise that you enable the most private security settings. When it comes to using photos as passwords, you will have to weigh the risks and benefits and decide if it is the best option for you. Maintaining control over your personal information is your responsibility, so stay informed, stay vigilant, and stay protected.