OUCH! January 2023

SANS SECURITY AWARENESS

OUCH!

The Monthly Security Awareness Newsletter for You

Biometrics – Making Security Simple

Overview

Do you hate passwords? Are you tired of constantly logging into new websites or can't remember all of your complex passwords? Frustrated by having to generate new passwords for new accounts or having to change old passwords for existing accounts? We have good news for you. There is a solution called biometrics that helps make cybersecurity easier for you. Below we explain what biometrics are, how they make your life simpler and why you will start seeing more of them.

First, Why Passwords?

Passwords are part of something called authentication, the process of proving who you are. There have typically been two things you can provide to prove your identity: something you know (like your passwords) and something you have (like an ATM card or your mobile device). Traditionally authentication has been done with passwords. Passwords were first adopted as it was one of the easiest authentication solutions to deploy. However, over the years our lives have become far more complicated with far more accounts than anyone ever expected. It is quite common for a person to have over 100 passwords in their work and personal life.

In addition, cyber attackers have become quite good at guessing, stealing or cracking passwords. This is why you see so many rules about passwords, such as making them long (so they are hard to guess) and using a unique password for every account (so if one of your accounts is hacked, your other accounts are still safe). The problem with all of the password requirements is they make being cybersecure more difficult. Password managers dramatically help as they securely remember all of your passwords and log you into websites for you, but is there a better way? This is where biometrics can help by providing a third thing to prove your identity – something you are.

Biometrics

Like passwords, biometrics are another way to prove who you are. The difference is instead of having to remember something (like your passwords) you use an element of who you are to prove your identity, such as using your fingerprint to gain access to your phone.

Biometrics are much simpler as you don't have to remember or type anything, you just authenticate using who you are. There are many different types of biometric such as your voice, how you walk, or your iris prints. However, fingerprints and facial recognition are the two most common, especially for mobile devices. While biometrics have a tremendous number of advantages, they also have some disadvantages, one of the biggest being if your fingerprint or face is copied by cyber attackers, you cannot change them.

Passkeys

Over the coming months and years, you should start seeing biometrics replacing passwords with a new technology called Passkeys. This technology is being adopted by Microsoft, Apple and Google and you should soon see it being adopted at more and more websites over time. Passkeys replace passwords by allowing you to prove who you are by simply using biometrics combined with your mobile device. When you create an account at a website (such as Google or Apple) instead of creating a password you register your mobile device. Moving forward you log into that website by authenticating with your mobile device using biometrics, such as your fingerprint or facial recognition. The website trusts your mobile device, and your mobile device confirms it's you using biometrics. In addition, your biometric data (fingerprint or face) is not sent to any website. Instead, your biometrics is securely stored locally on your device. It's just used to unlock the "Passkey", a unique key, created for each site, which your device sends to the site while protecting your biometric data. While no solution is perfect, biometrics and solutions like Passkeys can help keep you secure while simplifying security.

Guest Editor

Dr Johannes Ullrich is the Dean of Research for the SANS Technology Institute college. With over 20 years of industry experience, he currently monitors current threats by operating the SANS Internet Storm Center. He teaches SEC522 (Web Application Security) and SEC503 (Intrusion Detection).
Twitter: @johullrich & LinkedIn: https://www.linkedin.com/in/johannesullrich/.

Resources

Password Managers: https://www.sans.org/newsletters/ouch/password-managers/
More on Passkeys: https://www.sans.org/blog/what-is-phishing-resistant-mfa/