What are behavioral biometrics?

Amy Kover ⋮ 5-7 minutes ⋮ 11/15/2021

Technology has made it possible to do just about everything on your phone, from buying a car to filling a prescription. Yet, all of that ease has come with a side effect — passwords and more passwords. Security breaches and hacks mean that it's more important than ever that those passwords are more complex (your dog's name won't cut it anymore), and that you keep them all safe.

While password managers can offer a current solution, soon passwords may become a thing of the past as companies increasingly turn to behavioral biometrics as a new form of digital identification.

1. Being the only one of its kind.

2. Very special or unusual.

This technology tracks personal actions such as typing style and how you hold your phone, as well as habits such as the time of day you usually log in or your usual IP address. Algorithms then use that data to create a unique profile of you that is then used to verify who you are — or identify fraudsters. These capabilities can simultaneously help us access our accounts more easily while doubling down on security.

Here's what you need to know about behavioral biometrics:

How are behavioral biometrics different from physical biometrics like fingerprint and Face ID?

Like physical biometrics, behavioral biometrics make you the password, harnessing what makes you unique. Everyone interacts with technology in a different way, and behavioral biometrics identifies those patterns to create a profile that is almost impossible to replicate. The technology uses the sensors inside your phone or keyboard and mouse to measure how you move: How fast do you type? How much pressure do you apply to a touchscreen? At what angle do you hold your phone? Then it taps into device intelligence — your device's location or how it is connected to the internet — to measure against past behavior to detect abnormalities. When such abnormalities are detected, the software can raise alerts, lock the fraudster out of the account, block the transaction, and flag the activity to the account owner.

Why is there a growing interest in behavioral biometrics now?

Because fraud is changing and becoming more sophisticated. Fraudsters are constantly experimenting with new ways to circumvent security protocols, testing millions of usernames and passwords, activating teams of people to fill out CAPTCHA quizzes on websites and using more direct phishing campaigns to steal information. Behavioral biometrics can help identify fraudsters trying to pose as you online.

Let's say a criminal ring is signing up for accounts with a retailer to buy up a hot new product — like an Xbox or PlayStation — to sell on a secondary market. Biometrics technology would notice that the fraudster completes the registration process twice as fast as a genuine user. It would be able to tell if the fraudsters are "alt-tabbing" (a shortcut to switch between open programs), which isn't how people normally fill out forms, or they're cutting and pasting their name and address. Real users know that information from memory.

How accurate are behavioral biometrics?

On their own, behavioral biometrics will give a strong indication of whether the user is the right or wrong person. Combined with another form of validation, such as two-factor authentication, the results are very strong. For example, if 100 users sign up for an account on a retailer's site, behavioral biometrics can identify 60 of those who appear to be genuine humans because they're following all the same patterns humans follow, and they can be authenticated seamlessly. For the other 40, you can require a stronger form of authentication. This is where you implement additional security measures, such as requiring a scan of a driver's license — and how the bots will be uncovered.

Are my personal behavioral markers being shared with anyone?

No. Your behaviors are being evaluated by technology, which doesn't specifically know who you are. It doesn't know your name. It just knows the behavioral habits of the user coming from this location at this IP address, such as if this person typically gets their password wrong three times. It's then going to use that information to prevent a fraudster from sneaking into that account and ensure that only you are accessing your information.

Will behavioral biometrics eclipse passwords for good?

Right now, many organizations use behavioral biometrics in conjunction with passwords, but they are beginning to think beyond the password when it comes to stronger authentication. What we'll likely see for the near future is a layered approach with some friction — consumers seem willing to accept or even expect that in many cases, such as sending or receiving a large sum of money. In that example, a combination of passwords, behavioral biometrics and two-factor authentication, such as receiving a one-time passcode on your phone, may be warranted and even offer consumers more peace of mind. To log into your gaming app, behavioral biometrics, such as the device, location and time of day, may be enough. The method in which we authenticate ourselves will continue to evolve as the industry refines the balance between security and a great user experience.