Beyond passwords: Companies use fingerprints and digital behavior to ID employees

by Selena Larson @selenalarson

More companies are ditching passwords and using fingerprints and other biometrics to stop hackers.

"We're seeing a very rapid evolution from what used to be passwords, then smart cards, and now to biometrics," said Alex Simons, director of program management in Microsoft's identity division.

Biometric authentication uses face, fingerprint or iris scans to quickly confirm a person's identity. You probably already use itap by touching the home button to unlock your phone.

In the workplace, employees are increasingly using biometrics to log in to phones and computers, and to access data stored on those devices and in the cloud.

Spiceworks, a professional network for people in the IT industry, says nearly 90% of businesses will use biometric authentication by 2020, up from 62% today. Fingerprint scanning is currently the most common type of biometric authentication: 57% of organizations use it. Far fewer, just 14%, use facial recognition.

Companies such as Microsoft (MSFT) and Facebook (FB) are trying to get rid of passwords completely.

In 2015, Microsoft introduced Windows Hello with Windows 10. The new software uses face scans or fingerprints to log in to Windows devices. More than 50 million people use Windows Hello to log in to their PCs both in the home and at the office.

The Windows 10 Spring Creators Update will include a new authentication standard developed in collaboration with other tech companies, including Google. Called FIDO 2.0, the standard will enable Windows consumers to use multiple devices — including third-party security keys or a security monitors

that track your heart rate — to automatically log in to their computers without a password.

Related: Google's face match feature doesn't work in Illinois and Texas

"Passwords are the weak link. They have terrible characteristics about them, and they're hard for you to keep track of," Simons said. "Passwords are also super expensive for companies."

At Microsoft, Simons said he spends over $2 million in help desk calls a month helping people change their passwords.

Passwords are still widely used, of course, and one benefit is that they're easy to change if they're stolen. But you can't change your face or fingerprints, and biometrics can be stolen, too. In 2015, a breach at the federal Office of Personnel Management leaked 5.6 million people's fingerprints.

It's unclear for now what hackers can do with fingerprints. Experts worry that if they're adopted widely for authentication, it could lead to widespread identity theft. Researchers have already shown it's possible to use spoofed fingerprints to log in to smartphones.

Researchers have already tricked facial recognition by using a photo on older Windows devices and a Samsung smartphone.

Companies and consumers are also worried about third parties that are getting access to people's face scans through products like the iPhone X. Last year, Apple introduced facial recognition unlocking technology on the iPhone X and privacy advocates cited concerns about third-party companies having access to people's face scans. But the data shared with iOS developers reportedly can't unlock phones.

Meanwhile, Simons said biometrics collected with Windows are stored on the device directly and not shared to the cloud or with other third-party companies. Microsoft also provides the option to use a pin number instead of a biometric scan for anyone who is wary of sharing physical attributes.

State laws restricting biometric collection have hindered face and fingerprint-scanning tools or apps in some states. In 2008, Illinois passed a law that requires companies to let users know when biometric identifiers are collected

and how they will be used. It's also necessary to obtain consent from users before collecting and storing that data. In 2009, Texas passed a similar law. Data protection regulations about to go into effect in the European Union will also require consent before processing biometric data.

Biometrics will probably become just one part of a broader security strategy, perhaps as a second-factor login in addition to a password. Spiceworks' data shows just 10% of information technology workers think biometrics are secure enough to be the only form of authentication.

Other companies are using employee behavior to detect hacks.

Security firm BioCatch provides tools for companies to learn employees' digital behavior and identify when an unauthorized person is trying to access information.

Companies can add BioCatch software to apps and websites. It runs in the background to build a "behavior profile" of a user, and learns activities like how someone holds the phone, whether they type with one or two hands, and how they scroll or toggle between screens.

"The connected economy is forcing a need to redefine digital identity and to rely on new ways to make sure people are who they claim to be," said Frances Zelazny, vice president at BioCatch. "Your name and your pet's name, knowing that does not guarantee you really are a legitimate person."

Banks and the financial services industry are most interested in behavioral biometric technology. The Royal Bank of Scotland uses BioCatch.

People may be cautious about having their behavior tracked, but the trend toward biometrics should only grow.

"As we get better at explaining to the world how it works and as refine the software to make it easier to setup and use, more people are using it," Simons said. "Rather than trying to convince people that we're right, we're trying to give people options. We are trying to do everything in an upstanding manner to protect your privacy."

CNNMoney (San Francisco)First published March 18, 2018: 12:08 PM ET