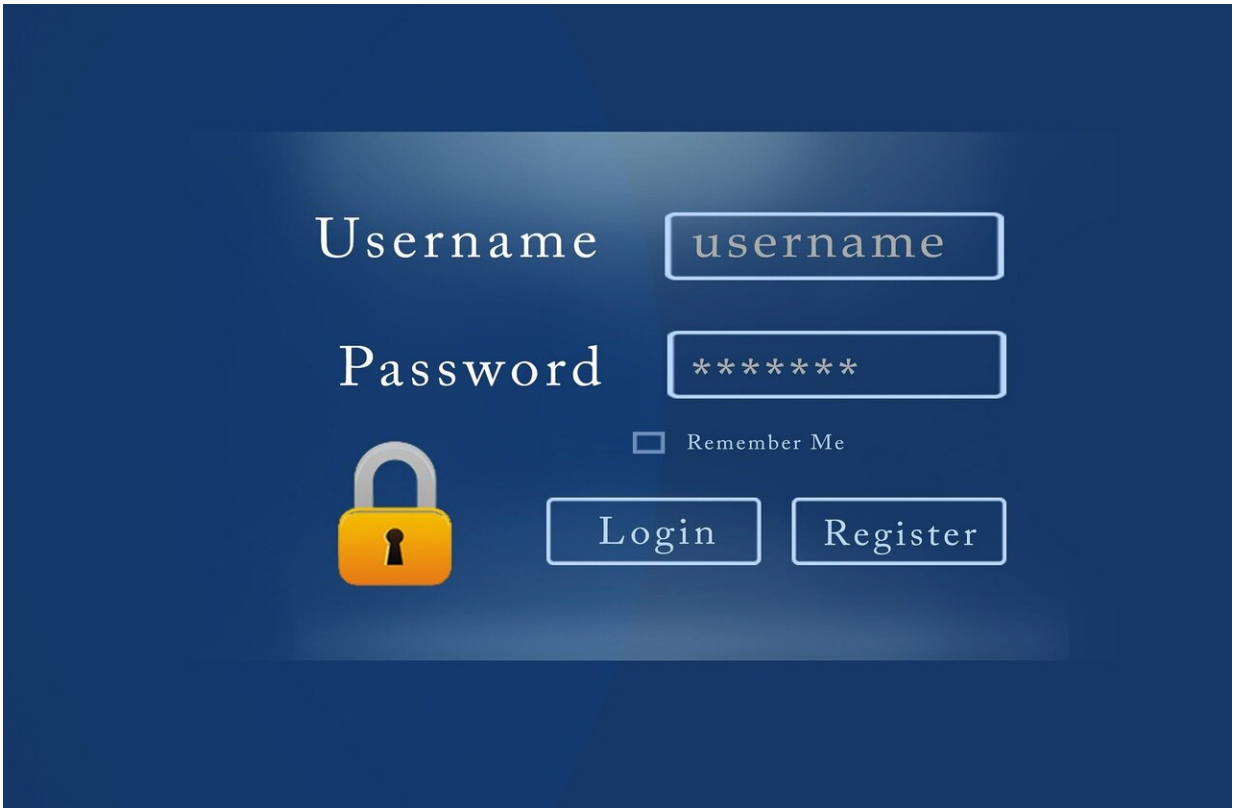
Dear passwords: Forget you. Here's what is going to protect us instead

March 3 2020, by Jessica Guynn, Usa Today



Credit: CC0 Public Domain

Do you hate remembering passwords? Soon, you may be able to forget them for good.

For years, we've relied on a secret we share with a computer to prove we

are who we say we are. But passwords are easily compromised through a phishing scam or malware, data breach or some simple social engineering. Once in the wrong hands, these flimsy strings of characters can be used to impersonate us all over the internet.

Slowly, we're kicking the password habit. With data breaches costing billions, the pressure is on to find more foolproof ways to verify someone's identity.

"We are moving into a world which we're calling passwordless, which is the ability for our applications, devices and computers to recognize us by something other than the old-fashioned password," says Wolfgang Goerlich, advisory chief information security officer for Cisco-owned security firm Duo.

Newer forms of identification are harder to imitate: something we are (such as the contours of our face or the ridges of our thumb) or something we have (physical objects such as security keys).

Intuit, for example, lets users sign into its mobile apps with a fingerprint or facial recognition or their phone's passcode instead of a password. Your fingerprint or screen lock can access some Google services on Pixel and Android 7+ devices.

Goerlich estimates that within five years, we could be logging into most of our online accounts the same way we unlock our phones. And then we will be able to finally break up with passwords for good.

What will replace them? That's a bit more complicated.

Any system that depends on a single factor isn't secure enough, according to Vijay Balasubramaniyan, CEO of Pindrop, a voice authentication and security company. Biometric information such as an

iris scan or a fingerprint can be stolen, too, and you can't change those.

Balasubramaniyan predicts several pieces of information will be used to verify identity. Machines will analyze our speech patterns or scan our fingerprints. We'll also be identified by something we have (our mobile devices, computers, key cards, fobs or tokens) and something we do (our movements and location, our behavior and habits, even how we type).

If that seems more invasive than sharing some random bits of knowledge such as our mother's maiden name or a PIN number, it is. But Balasubramaniyan argues these trade-offs are necessary to shield our personal information in a hyper-connected world.

"It's going to be scary," he says, but, "it's time for consumers to demand a higher level of privacy and security."

Password overload

Secret words to tell friend from foe have been around since ancient times and, in the early days of the internet, they made a lot of sense.

We started out with just a handful of passwords to access our email, a few e-commerce sites, maybe an online subscription or two. But soon, we were transferring our entire existence into the cloud, storing our medical and financial information, photos of our kids and our innermost musings there.

And every time we clicked a link or downloaded an app, we had to come up with another password. As even more devices connected to the internet, from home surveillance systems to thermostats, we hit password overload.

Today, people have an average of 85 passwords to keep track of,

according to password manager LastPass. Our brains just aren't wired to squirrel away unique passwords for so many online accounts. So we reuse and share them. We jot them down on Post-Its or in Word documents. We sign in with Facebook or Google. We shell out a few bucks for a digital password manager.

But data breaches keep proliferating. So we're told to conjure up stronger passwords, the longer and more random the better (use special characters!). We're prodded to enable two-factor authentication. And we grumble so much about it all, our collective frustration has turned into a popular internet meme: "Sorry your password must contain a capital letter, two numbers, a symbol, an inspiring message, a spell, a gang sign, a hieroglyph and the blood of a virgin."

Turns out the only fans of passwords are hackers and identity thieves. Even researcher Fernando Corbató, who helped create the first computer password in the early 1960s, was a detractor before he died.

Corbató told the Wall Street Journal in 2014 that he used to keep dozens of his passwords on three typed pages. He called the current state of password security "kind of a nightmare."

"Passwords are a 60-year-old solution built on a 5,000-year-old idea," says Jonah Stein, co-founder of UNSProject, which allows you to access your accounts using the camera on your phone. "Daily life demands that we create and remember a new password for almost every single thing we do—reading the news, paying bills, or simply ordering a pizza. The promise of online convenience has been broken by antiquated authentication solutions with unrealistic security best practices."

Are we really over passwords?

So will passwords finally go the way of the eight-track tape? For years,

reports of their demise have been greatly exaggerated. Tech leaders have dangled but never delivered on promises to eliminate passwords.

"There is no doubt that, over time, people are going to rely less and less on passwords," Microsoft's billionaire founder Bill Gates told the RSA conference in 2004. "People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure."

So what's taking so long? Too many options being floated and too little consensus on what will work best.

Companies, eager for our eyeballs and our business, are holding out for solutions that strike a balance between convenience and security. With security costs skyrocketing and consumer trust flailing, the industry is under growing pressure to lock down our accounts, security experts say. By 2023, 30% of organizations will use at least one form of authentication that does not involve a password, a significant increase from the 5% today, according to research firm Gartner.

One of the major proponents of a password-free world is the FIDO Alliance, which stands for Fast Identity Online. The consortium of heavyweights from Google to Microsoft is developing technical standards to verify identity. Apple recently joined the FIDO Alliance, giving the group even more clout.

We can't ditch passwords overnight, but, according to Andrew Shikiar, executive director of the FIDO Alliance, "the imperative is there now."

"Businesses are feeling these pain points and they are being pushed to come up with solutions that are not dependent on the old ways of authenticating," he says.

That the industry is working arm in arm on solutions is "really unprecedented," Shikiar says. "This sort of collaboration is a very good sign that, not only is there a way to go past passwords, there is a will."