

## The End of Passwords

*The era of passwords may be waning. The “passkey” concept should make account logins quicker and safer.*

I probably have over 200 passwords stored in the 1Password company’s cloud servers. They’re safe and easy to look up, but managing these pieces of flotsam and jetsam is a pain.

Fortunately, there’s help on the horizon!

But before we go there, let’s talk about authentication—for instance, how does Amazon know it’s you who is ordering a gross of Crest Toothpaste?<sup>1</sup>

Online web accounts ask for two pieces of information (we call them “keys”) to confirm that you are you:

1. **An ID**, like your email address, is a “public” key that you give out willy-nilly to scads of people and websites. This is how a website knows who’s knocking at its door (so to speak) and where to send you emails. Email addresses make good IDs because they’re unique, and, like your street address, they’re public so folks can find you. On the other hand, you don’t want the bug man<sup>2</sup> walking in your front door, so you keep it locked with a private key on your keyring.<sup>3</sup>
2. **A password** is the private “key” you use to complete your online authentication. (This means you shouldn’t use the same password for every website, just like you don’t use the same key for your house, car, and safe deposit box at the bank. And that’s why I have 200 passwords.)

### Two-Factor Authentication

Over the past few years, some websites—especially banks—have added two-factor authentication to their login process. After you enter your ID and password, the bank sends you a text message with a one-time numeric string. When you enter that number, the website has authenticated you on TWO devices—your computer and your smartphone (or tablet). (If you don’t have a smartphone, you can opt to have the website call your phone and recite the numeric string you’ll type in).

### “Biometric” Identifiers

Unfortunately, no matter how many “keys” and codes we have to enter, IDs and passwords are just text characters that can be stolen, forgotten, or accidentally sent in response to a phishing email.

Fortunately, most of us have two unique identifying traits that can’t be replicated: our face and fingerprints. Many newer mobile devices and laptops already use face ID or fingerprint (“biometric”) sensors to ensure that the actual owner is using that device.

I have an older iPhone that uses my previously stored fingerprint to “wake up” the phone and authenticate me as its rightful owner.

Now that I’ve authenticated myself on my iPhone, there should be a way the phone can authenticate me to the website I’m visiting.

### Passkeys

And that’s what passkeys do. Apple, Microsoft, and Google are major players in implementing the FIDO (Fast IDentity Online) alliance’s protocols that can use my smart devices’ biometric authentication to encrypt my login IDs into what are called “passkeys.”

Once a website has adopted the FIDO standard, it will accept my passkey from my smartphone, tablet, or computer and then automatically admit me to the website. There’s no password to remember—or forget—or lose.

Apple is implementing Passkeys on its newest operating systems this fall (MacOS Ventura, iOS 16, and iPad OS 16). Google will add Passkeys to Android devices by the end of this year. Microsoft is aiming for 2022–2023 with Windows 11 updates.

I suspect websites will adopt the passkey protocol sooner rather than later to ensure their client’s data is secure and make ordering toothpaste even easier.

### If You Need Help

Remember, if you need tech help, just fill out one of our tech help requests at <https://princetonior.wufoo.com/forms/technology-assistance-request/>.

<sup>1</sup> Recommended by nine out of ten dentists, many of whom own stock in the Crest Toothpaste Company. I’m not sure what the tenth dentist uses.

<sup>2</sup> We have a nice bug man who comes by every few months and looks for bugs. He then tells us if he finds any.

<sup>3</sup> I keep my keys in the refrigerator because that’s where I’ll often find them.