

A Password Reprise, and Hope on the Horizon

AUTHOR: ZACHARY MERKLE

A few years ago, we wrote about the importance of [strong, secure, unique passwords](#). Using a weak password, particularly one that is shared across multiple services, provides an easy avenue for a data breach. Professionals are particularly at risk because they maintain client data — if a professional firm suffers a data breach, its clients are at risk too. It is not hard to see the potential for liability. While professionals should hold [cyber liability insurance](#), insurance cannot protect from reputational damage from getting hacked, the headache that accompanies a data breach, and the increased premiums arising from claims on said policies.

Creating and remembering these unique passwords is easier than ever. Many organizations offer password managers for their employees to use. [Third-party password managers](#) are available for purchase, both personally and for businesses. And nearly everyone owns a smartphone running iOS or Android; [Apple](#) and [Google](#) maintain their own built-in password managers.

Even with these helpful tools, passwords are a chore. We get it. But there might be hope on the horizon: passkeys.

For those unaware, the biggest technology companies have been working together on this new standard. These “passkeys” authenticate your logins (websites, services, etc.) directly from biometric data, such as the fingerprints and face scans that already unlock your trusted devices. The security experts find that these passkeys are less susceptible to common hacks than passwords. And passkeys are easier to use because logging into your service of choice is as easy as scanning your face or fingerprint on your phone. No more managing a database of unique passwords for each website.

Look out for passkeys to start becoming an option for your logins — [Microsoft](#), [Google](#), and [Apple](#) have already started adopting them, with more companies surely to come. Professionals on the forefront of internet security will better protect client data and shield themselves from liability. Passkeys may soon let professionals ditch passwords while *increasing* their security. A win-win.