Passwords Are Getting Ridiculous, Right? Consider Simplifying Your Company's Two-Factor Authentication With A Physical Security Key

Benjamin Jackson
bjackson@mwlaw.com
(501) 688.8887

09/20/2018

If you clicked on this post, that means you probably fall into one of two categories. Category 1: You are really tired of having to come up with – and remember – increasingly more complicated passwords, only to then be asked for a second-level passcode. Category 2: You are responsible for your company's data security and you are really tired of hearing people whine and complain about how complicated their computer login process has become.

Passwords have gotten so complicated these days that essentially everyone who has a job involving a computer falls into one or both of those categories. In fact, all these special characters, capital letters and numbers have led to a multi-million dollar industry for apps that will hold all your complicated passwords. But wait, you need a password for that, too!

What is the result? According to Verizon's Data Breach Investigations Report (DBIR) for 2018, 40 percent of data breaches occurred due to lost passwords. Employees can't remember them all, so they end up written on notes, stored in phones and laptops, and who knows where else.

As a result, most companies are now moving to an extra layer of security on top of the standard password, like sending you a text or e-mail, or using an authenticator app to generate a code you have to enter before you can access your account. What is next, three-factor authentication?

We all know data security is extremely important, and that the battle to stay ahead of hackers, as well as other information security threats both within and without your company is of the utmost importance. But even cybersecurity attorneys like us recognize that all this security can be a real drag for the every day employee.

One answer to help simplify this whole process may be physical security keys. Actual, physical USB "keys" that you insert, tap or touch to your computer or device to obtain access without the need for a password or authentication code. There are also Bluetooth variations, although recent concerns, such as a warning from the U.S. Computer Emergency Response Team that Bluetooth devices contain vulnerabilities to hackers, may make those a bit more risky at this stage.

The idea is that the keys serve as a simpler form of two-factor authentication. Actually, for personal use the keys could ultimately eliminate the need for passwords altogether. That may be the endgame for companies, too (wouldn't that be great!), but does not seem to be the selling point so far. There is, however, real potential that with sustained success physical security keys could reduce the complexity of

your required password, as well as how frequently you have to change it, and eliminate the need for a second-factor text, e-mail or app with yet another code to enter.

This year, Google announced that using a physical security key in its workplace had reduced the number of Google work accounts that had been compromised to zero. You read that right. Zero. Google has 85,000 employees. That's a pretty good test case. As of this month, you can now buy your own set of Google Titan security keys for $50.

Microsoft, in a partnership with the Fast Identity Online (FIDO), an alliance representing 250 organizations from various industries seeking a secure alternative to passwords, to create the Yubico key for use with Windows Hello. Yubico keys range from $20 to $50 on Amazon as of this posting.

Of course, there will always be drawbacks. Employees may find themselves locked out of the system temporarily when they lose the key or leave it at home. And your IT department will *love* all the questions like "now where am I supposed to carry *this*" when the keys are issued. But overall, a simplified tool that (so far) has the potential to dramatically reduce data breaches from outside the company, and directly sources those that occur from within, has a lot of potential.

So there it is - we may have come full circle. Remember that key your dad (granddad?) had to his desk for sensitive documents? Well, this is kind of like that only fancier. And maybe less sketchy-looking. There is a chance physical security keys are the path to fewer "password update" reminders, and that someday we can all forget where that {@$# special character key is.