CPA
Practice Advisor

records, and bank account and credit card numbers. Even password managers don't eliminate ...

Jim Boomer • Nov. 20, 2017

Think of all of the passwords you manage right now. How many of them are written down? Do you use the same password for multiple websites? We know these actions put our data at risk, but we do them anyway because otherwise, we couldn't possibly remember the hundreds – if not thousands – of passwords we'd need to memorize for all of the apps, devices and websites we use in our personal and professional lives.

It's not hard to see why people don't like passwords. We share a lot of sensitive

years ago, those alternatives were rare and expensive to adopt, but today the shift away from passwords is accelerating. So let's take a look at the options out there.

Multi-factor authentication

I covered multi-factor authentication in detail for this space recently. While multi-factor authentication often uses passwords, it also requires one or two additional pieces of information. Strong authentication requires two or more of the following:

1. **Something you know.** A password, PIN or answers to previously established security questions.
2. **Something you have.** A physical object in your possession, such as a token or text-enabled phone.
3. **Something you are.** Biometric features such as a fingerprint.

Biometric authentication

I touched on biometric authentication above, but it involves much more than just a fingerprint. Facial, voice recognition and iris scanners are the most popular methods after fingerprints. But companies are experimenting with many more biometric authentication methods to replace passwords, including heartbeat recognition, vein recognition, hand and finger geometry,

One-time passwords

One-time passwords (OTP) are an authentication mechanism that uses non-persistent passcodes that are valid for only one session. For each login attempt, a passcode is generated and sent to the associated phone number or email address. The user has to enter the passcode to access the account, and it is only valid for the duration of one session. Subsequent logins require a new passcode.

Picture passwords

as they were originally performed.

While each of these technologies has their own benefits and pitfalls, almost everyone agrees that passwords alone are too insecure for modern use. Our digital world requires more privacy and security than passwords can provide. We'll likely see a decline in password use in the next few years as alternatives supplement or replace them.

Firm Management • Security