A Solution to the Password Problem

Presented by Kevin & Kyle Taylor

Whether you're looking to make a New Year's resolution or you're simply trying to implement some information security best practices, you would be well served to start using a password manager. Why?

Passwords: The weak link

According to a survey by Digital Guardian, "password overload" is a real problem. Worse, despite known risks, at least half of us admit to reusing passwords.

How many online accounts do you have? Probably more than you think. You've likely got at least one social media profile. Then, there's your e-mail (which might include both personal and work accounts), your various banking accounts, streaming services like Netflix or Hulu,

and your Amazon account (who doesn't have one of those?!). That's not to mention all those apps on your smartphone.

Now think about the passwords you use for those accounts. Chances are, either you reuse passwords across multiple accounts or you have your passwords written down somewhere—both of which are no-nos when it comes to information security best practices. If, as the experts tell us, you need a strong password for each account that is at least eight characters long (and preferably longer) and combines upper- and lowercase letters, numbers, and symbols, there's simply no way you can remember all the passwords to all your accounts.

Unless, that is, you start using a password manager.

An all-in-one solution

A password manager—some well-known versions include LastPass, Dashlane, RoboForm, and 1Password—is essentially a secure online storage vault for your passwords. You'll find both desktop and smartphone app versions available. Load them on multiple devices and your information will be synced across them.

There are several features that make password managers extremely valuable from an information security standpoint:

1. **Remember one master password.** Because the password manager stores all your credentials for you, the only password you need is the one that logs you in to the vault. So be sure to make it the most complex password you can think of—and remember!
2. **Auto-generate passwords.** Instead of trying to come up with a unique, complex password for each account on your own, the password manager will do it for you—and save it for future use.
3. **Automatically save and store new accounts.** Adding a new streaming service? Opening a new credit card or bank account? Your password manager will recognize the new account and save your credentials for you, so your next login will be seamless.
4. **Easily fill web forms.** By saving some of your personal information in the vault (e.g., address, phone number, and credit card number), the next time you have to fill out

an online form, the password manager will auto-fill your information. It's safer than storing these details in your browser.

5. **Log in to sites automatically.** Once your preferred sites and credentials are set up, you can access the sites directly from the password manager, which will log you in automatically. As an added bonus, with the browser extension enabled, you can navigate to the website you want to visit, and your password manager will log you in—again, automatically.

Hopefully you're seeing how much easier—and more secure—your online life can be. Imagine never having to remember multiple passwords or having to go through the hassle of resetting your password because you forgot it. That's what a password manager can do for you.

Ready to get started?

First, find the one you want. PCMag has put together this side-by-side comparison of what it considers the best password managers of 2019. Ranging from the most expensive (Dashlane, at $59.99/year and climbing) to the least expensive (Zoho, at $12/year), you'll also see the various features each of these tools offers. You might consider one of the free password managers available, which PCMag also reviews.

Once you download the manager you want, you need to start adding your accounts. Keep in mind that this can be time consuming, depending on how many accounts you have. Don't worry if you miss a few on this first pass; you can always come back later to add more. This is where the password manager earns its keep. You'll be able to see, at a glance, which existing passwords are considered weak, as well as which ones are repeated across accounts. From there, simply use the tool's password generator to create and assign new, unique passwords to these accounts to shore up your online security.

Be sure to enable multifactor authentication (MFA). An extra layer of security, MFA will require you to provide two forms of identification to log in to your password manager—your password and a second token, which is typically a passcode sent to your smartphone or an authenticator app. Considering how much sensitive information will be stored in the tool, *this step is a must*.

Now, all you have to do is monitor the passwords you have saved. Many password managers alert you when it's time to refresh your passwords (which you should do periodically). Some, like Dashlane, even scan the dark web for risks to your personal information.

What are you waiting for?

You may have had your personal e-mail account hacked, all because you used a weak password that was easy for some cybercriminal to guess. Or maybe your credit card number was stolen from an online payment site, again due to weak credentials. You might argue that a company like Dashlane or LastPass can get hacked, too, so why bother going through this hassle? In fact, LastPass was hacked, back in 2015, but the exposed data was encrypted, so the hackers didn't really get away with anything.

The lesson? No account is completely hack-proof, but using a password manager can substantially reduce the risk that your passwords—and the information secured behind them—will be compromised. And that's an information security best practice you want to follow, in the New Year and beyond.

Authored by Kate Flood, director, editorial, at Commonwealth Financial Network®.

Kevin Taylor is a financial advisor located at Vaughn Wealth 1127 Edgewater Drive, Orlando, FL 32804. He offers securities and advisory services as a Registered Representative and Investment Adviser Representative of Commonwealth Financial Network®, Member FINRA/SIPC, a Registered Investment Adviser. He can be reached at 407-872-3888 or at Kevin@vaughnwealth.com.

Kyle Taylor is a financial advisor located at Vaughn Wealth 1127 Edgewater Drive, Orlando, FL 32804. He offers securities and advisory services as a Registered Representative and Investment Adviser Representative of Commonwealth Financial Network®, Member FINRA/SIPC, a Registered Investment Adviser. He can be reached at 407-872-3888 or at Kyle@vaughnwealth.com.

Vaughn Wealth | 1127 Edgewater Drive, Orlando , FL 32804