SUFFOLK COUNTY BAR ASSOCIATION
NY
1908
1908 100 Years of Progress 2008

THE SUFFOLK LAWYER

THE OFFICIAL PUBLICATION OF THE SUFFOLK COUNTY BAR ASSOCIATION

VOL. 35, NO. 1 - January 2020

DEDICATED TO LEGAL EXCELLENCE SINCE 1908

WWW.SCBA.ORG

Should Lawyers use password ‘managers?’

By Victor Yannacone, Jr.

Victor Yannacone, Jr.

Password managers make it easy to use strong, unique passwords everywhere and help protect you from imposter websites trying to “phish” your password.

Password managers store your login information for all the websites you use and help you log into them automatically. They encrypt your password database with a master password which will be the only one you have to remember.

Don’t reuse passwords!

Password reuse is a serious problem because of the many password leaks that occur each year, even on large websites. To prevent a password leak on one site from compromising your accounts on other sites, you need to use unique, strong passwords on every website — long, unpredictable passwords that contain numbers and symbols.

Using a password manager

After you have logged into your password manager with your master password (the only one you will have to remember), just log into a website and your password manager will automatically fill in the data for you. You don’t have to remember what email address, username, and password you used for that website. It can also be configured to automatically fill information like your address, name, and email address into web forms.

When you create a new account, your password manager will offer to generate a secure random password for you’

Browser-based password managers aren’t ideal

Although the major web browsers — Chrome, Firefox, Internet Explorer, and others — all have integrated password managers they can’t compete with dedicated password managers.

A dedicated password manager will store your passwords in an encrypted form, help you generate secure random passwords, offer a more powerful interface and allow you to easily access your passwords across all the different computers, smartphones and tablets you use.

Password managers to use

A variety of password managers are available. Here are the most popular but when deciding which to choose you will need to consider what features are more important to you.

Dashlane[1] operates on almost every platform — Windows, OS X, iPhone, iPad, and Android with extensions for every browser, and features like a security dashboard that analyzes your passwords and an automatic password changer that can change your passwords for you without having to deal with it yourself. It is free to use on a single device but requires a paid upgrade to sync your passwords between multiple devices.

Dashlane lets you choose to keep all of your passwords locally on your computer, rather than in a cloud. If you do choose to sync your passwords using the cloud, they are AES encrypted.

LastPass[2] is a cloud-based password manager with extensions, mobile apps and even desktop apps for all the browsers and operating systems. It offers a variety of two-factor authentication options and stores your passwords on LastPass’s servers in an encrypted form. The LastPass extension or app locally decrypts and encrypts them when you log in, so LastPass couldn’t see your passwords if they wanted to.

KeePass[3] is a popular desktop application with browser extensions and mobile apps. It stores your passwords on your computer and is open-source, however, you have to sync passwords between your devices manually.

1Password[4] and **Bitwarden**[5] are other open source alternatives to KeePass.

On modern devices, you can also unlock your password manager vault with biometric authentication like Face ID or Touch ID on iPhones.

While you do have to place some trust in

(Continued on page 25)

Cyber (Continued from page 12)

whatever password manager you choose, using a password manager is more secure than the alternatives.

Your master password

The master password which controls access to your entire password manager database, has to be particularly strong. It's the only password you'll need to remember. You may want to write down the master password and store it somewhere really safe. You can change this password later, but only if you remember it. If you lose your master password, you won't be able to view your saved passwords which is why no one else can either.

After installing a password manager, you can start changing your existing website passwords to more secure ones the next time you visit each site.

Peace of mind when logging in

Your password manager doesn't just make it faster to enter your credentials while browsing the web. It gives you peace of mind while it goes about its job.

If you're signing into your email online, you don't need to double-check the domain before typing your username and password. You know that if your password manager is offering to fill your credentials automatically, it's already checked that the domain is a match with the one saved in your database.

This works on smartphones, too. Use your password manager to enter credentials and you'll be protected from phishing on the mobile web too.

How a password manager helps protect you

If you use a password manager you have additional protection against phishing as long as your password manager automatically fills your credentials.

If you save a login for a website like your bank or credit card, your password manager will remember it and offer to automatically fill it in for you when you log on. If you end up on a phishing website that looks like your intended website, your password manager won't offer to enter your credentials. Your password manager doesn't fall for the disguised URL. When your password manager refuses to complete a login you shouldn't either.

Note: Victor John Yannacone Jr. is an advocate, trial lawyer, and litigator practicing today in the manner of a British barrister by serving of counsel to attorneys and law firms locally and throughout the United States in complex matters. He has been continuously involved in computer science since the days of the first transistors in 1955 and actively involved in design, development, and management of relational databases. He pioneered in the development of environmental systems science and was a cofounder of the Environmental Defense Fund. He can be reached at (631) 475–0231, or vyannacone@yannalaw.com, and through his website https://yannalaw.com.

[1] https://www.dashlane.com/lp/search?utm_source=adwords&utm_campaign=US_Search_Brand_Exact&utm_medium=15594053097&utm_term=Dashlane&gclid=EAIaIQobChMIguHjpc_K5gIVRR6tBh3h1gEWEAAYASAAEgIUQPD_BwE

[2] https://www.lastpass.com/get-premium?&gclid=EAIaIQobChMIqd6x6M7K5gIVkeNkCh1aWAJ2EAAYASAAEgJ5_PD_BwE

[3] https://keepass.info/

[4] https://1password.com/?gclid=EAIaIQobChMI3a6FxtDK5gIVGP5kCh3QJwJYEAAYAiAAEgIMDPD_BwE&gclsrc=aw.ds

[5] https://bitwarden.com/