nLightenedThoughts

April 2018

William Blinn Communications
Worthington, Ohio 43085
www.blinn.com • 718.577.1054

Why You Need a Password Management Strategy

Browsers have never offered a secure way to store passwords and the situation became a bit more dicey recently when the developers of a password recovery tool added some new features.

Password recovery tools aren't new, but the LaZagneForensic utility's new features make it dangerous in the hands of the wrong people. The utility is freely available on the internet via GitHub. The LaZagne project is an open source application used to retrieve passwords stored on a local computer. The developer says the tool "has been developed for the purpose of finding these passwords for the most commonly-used software."

System administrators need utilities like this because users sometimes forget the passwords that they have created to protect essential information. In the past, there's been little risk because they required physical access to the computer. That's no longer necessary in some situations.

If you have a Mac and you're now relaxing because this specific problem doesn't affect you, please continue reading because there are other reasons why storing passwords in browser is a bad idea.

Password managers such as LastPass, 1Password, Dashlane, and others provide benefits beyond simple password storage.

On January 13, 2018, the Hawaii Emergency Management Agency mistakenly sent an alert that went to cell phones, radio stations, and television stations. For nearly three quarters of an hour, residents of Hawaii thought a missile was heading their way. It took 38 minutes for the agency to send a correction.

Why? They knew immediately that the alert was incorrect, so why didn't they just send a correction?

Cause #1: They had no system in place for sending a cancellation message.

Cause #2: Hawaii governor David Ige, who could have issued an immediate correction on Twitter couldn't do so for 17 minutes because he couldn't *remember* the password.

Password Complexity

Have you ever created a password so memorable that you know you'll never forget it and yet, 10 minutes later, you're unable to recall what it was?

Some people eliminate that problem by using the same password for everything, but that creates an even more serious problem: Someone who manages to obtain your Facebook password will also have the password you use for your email account, your on-line store accounts, and your bank.

Other people think they have solved the problem by writing their passwords on sticky notes that hang from the bottom of the computer screen. At least one photograph taken at the Hawaii Emergency Management Agency shows exactly that. Most people realize that sticky notes are not good places for passwords. So if every password needs to be different and you can't write them down, how are you supposed to remember them?

That's what a password manager is for.

With a password manager, you need to remember only one password. It is important for this password to be strong, but memorable. You can leave some clues as memory aids if those clues are sufficiently obscure that nobody else will be able to decode them.

nLightened Thoughts (ISSN 1543-1533) is for clients and friends of William Blinn Communications, Worthington, Ohio. Phone 614.785.9359 (Columbus) and 718.577.1054 (NYC). On the Web at www.blinn.com.

Creating a Password Clue

What if someone saw this on a sticky note hanging from your computer screen?

Would that hypothetical someone know how to decode this?

- **84** = Denver (because that's where you lived in 1984).
- **home #** = 2375 (because that was your home town street address number).
- **excited** = ! (well, that one should be obvious).
- **kitty** = Tiger (because that's the name of your favorite cat).
- **BiL** = RmA (because Richard Mark Allen is your brother in law).

The password this would be a clue for is **Denver2375!TigerRmA**.

The result is an extremely secure password that can be hinted at with clues left in plain sight. Create your own formula instead of using this one to establish memory triggers that only you will recognize. Avoid any current information that others might know (spouse's name, pet's name, house number, phone number, and so on). Pick clues from the past — and further back is better.

Avoid Bad Passwords

Security experts suggest many people use astonishingly insecure passwords.

Examples: 123456, password, admin, qwerty (or azerty), abc123 (or AbC1@3), 123123 (or 123!@#), letmein (or LetMeIn or 1eTmE1n), password1 (or pa55Word!), and trustno1.

These are some of the absurdly insecure passwords people have used. Even a password manager won't help if you use passwords like these. But that's another big advantage of using a password manager. Except for the master password, all other passwords can be utterly impossible to guess.

Example: **#5B3g4^c9GHACD%sgb**

Using current technology, this password is not crackable because it's 18 characters long and includes upper and lower case letters, numbers, and symbols. Reduce that to 9 characters and the time to crack it would be less than 1 day. The oh-so-clever "1eTmE1n" would be cracked in less than a day. Passwords like "123456" and "password" would last only a few seconds. (The password analysis was provided by *http://www.passfault.com/*.)

How long it might take to crack a password is a matter of considerable debate, but it's safe to say that any password that's crackable in less than a week is useless. One analyst's "2 days" might be another analyst's "0.2 seconds"; it depends on the amount of computing power applied.

As early as 2013, a team of hackers had managed to crack more than 14,800 supposedly random passwords from a list of 16,449 as part of a hacking experiment. (Source: *London Daily Mail*) So passwords of 18 to 20 characters are not unreasonable for data you want to be absolutely secure.

LastPass is the password manager I use. It works with all browsers as well as Android and IOS devices. Other password managers such as 1Password and Dashlane have similar capabilities, so it's more important to install a password manager, regardless of which you choose.

Browsers Store Passwords

All modern browsers (Chrome and Firefox, for example) will offer to save passwords and fill them in automatically when you next visit the site. Password managers are better.

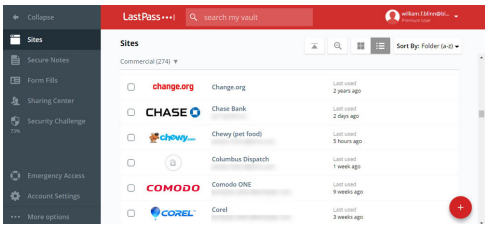
This information draws on my experience with LastPass, but expect similar functionality with the other apps.

Passwords are not stored in a single location. The password manager stores data locally (encrypted), on its central server (encrypted), and synchronizes the encrypted passwords to all other browsers on all other computers and mobile devices you use. So if you need a password urgently (and only your cell phone is available) you'll have access to it.

The password manager will be protected by the master password that only you have. Even the password manager's developer has no access to that password. Encryption is typically based on your master password and, if you change it, your stored passwords will be re-encrypted.

LastPass uses AES 256-bit encryption. When passwords are decrypted, the process occurs on your local machine. The company uses salted hashing and PBKDF2 implemented with SHA-256. These are complex processes that protect the master password and encryption key against large-scale, brute-force attacks.

A password manager may allow you to share specific passwords with others, to set up sub-accounts, and even to name another person who will be allowed to access the data in certain circumstances.



Many password managers offer additional functions, such as providing the ability to securely store information such as Social Security numbers, license numbers, account numbers, and other information that you'll need but shouldn't be stored in an unencrypted file on the computer.

You'll probably also find a password generation feature that will create a hard-to-crack password when you set up an account on a new site. Many of these applications also store information that you may need to fill in to on-line forms. This feature can save quite a bit of time in addition to maintaining the information in an encrypted file.

LastPass even offers a security challenge that reviews passwords to find weak, duplicate, and potentially-insecure passwords. It also warns if you have an account on a website that has recently suffered a breach.

The time to install a password manager is now, not after losing data to a breach. Ω