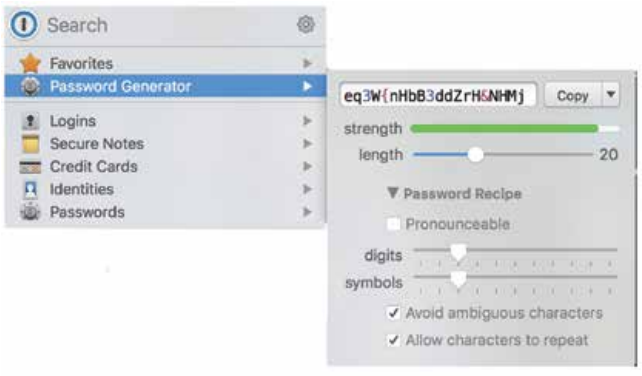
Managing Passwords

LifeInNaples • December 30, 2015



It was just a few years ago that you could use the same password for everything, do you remember those days?

Since I last wrote about managing passwords in 2013, the world has changed its views of password management. Some of the password and security breaches that have been revealed in the past few years included large entities like Facebook, Target, LinkedIn, Google, Yahoo! and Twitter to name just a few.

THERE ARE TWO BASIC RULES FOR PASSWORD MANAGEMENT IN TODAY'S WORLD

1. The password must be complex and difficult to guess.

2. The password must be easily remembered.

While the first rule is necessary, the second is nearly impossible with the complex passwords that are becoming the norm. I will give you some tips on how to implement both rules without losing your mind.

Whenever there's a big data breach and user passwords are exposed, security companies always make a list of the most common passwords people were using. The five most common passwords of recent breaches were "123456," "123456789," "password," "password123," and "12345678."

Obviously, you shouldn't use those or anything similar, but millions of people still do! The same goes for special dates; names of spouses, children, sports teams, relatives or pets; or any password using the full name of the service you're making the password for. (such as 'amazon1234')

Despite what you see in the movies and on TV, professional hackers never sit down at a computer and try to guess your password. Instead, hackers get millions of passwords at once from company data breaches or other sources. Usually these passwords are 'hashed' so they're just a huge string of letters and numbers. However, if enough passwords are 'hashed' the same way, hackers can figure out the pattern and decrypt many of them. In fact, with modern computers, they can usually crack tens of thousands of passwords in a matter of hours.

Use a different password for each of your important accounts, like your email and online banking accounts. Reusing passwords is risky. If someone figures out your password for one account, that person could potentially gain access to your email, address, and even your money. Your email should also have it's own unique password as if a hacker gets access to this, they can use it to "reset" your passwords from your other accounts.

Using numbers, symbols and mix of upper and lower case letters in your password makes it harder for someone to guess your password. For example, an eight-character password with numbers, symbols and mixed-case letters is harder to guess because it has 30,000 more possible combinations than an eight-character password with only lower case letters.

Now, if you're like me and have dozens of accounts online, even using this system can be too much. That's why a password manager like 1Password can be a great help. It keeps your passwords secure, and you only need to

remember the one to open it. Plus, it's a local program so you aren't uploading your passwords to the Internet, and they can also be securely kept on your portable devices if you choose. 1Password also has a great random password generator that will create a complex password and remember it for you!

Don't leave notes or books with your passwords to various sites on your computer or desk. People who walk by can easily steal this information and use it to compromise your account. If you decide to save your passwords in a file on your computer, create a unique name for the file so people don't know what's inside. Avoid giving the file an obvious name, such as "my passwords." Also do not put the name 'password' in the text of the file, as a manual search of the computer can easily turn up those lists! It is also a bad idea to choose the option to save your password when visiting Web sites or setting up an e-mail client — it is much more secure to enter the password again each time you visit.

An alternative to using a "password" is to use a "passphrase." A passphrase is a sequence of words strung together to create a "password." To do this, you need to forget your traditional methods for building a password. Instead of worrying about how many characters your password needs to have, consider multiple words that can be combined to make a phrase. A passphrase is made up of four or five short words, put together in a way that makes sense to you.

While your "password" may be longer (which makes it more secure), it will be easier for you to remember. Here are some examples:
"My dog just turned eight." = "MyDogJustTurn-D8"
"Look at all the traffic today!" = "LookatAlltheTraffic2day!"
"I love to go fast in my Tesla!" = "Ilove2goFastInMyTesla!"

Passphrase's should meet all of the requirements of traditional passwords. You should choose a phrase that you can easily remember; and to increase security avoid common phrases, lyrics, titles, and quotations.

Paraphrasing is another easy way to form a secure password that you can easily remember, it is to think of a phrase, song, poem, or sentence and use the first letter from each word. For example: “I have owned my dog for 5 years!” = “Ihomdf5y!”

Passwords do not have to be a nuisance if you devise a good plan to manage them!