239.595.0482 jeff@jeffbohr.com

MANAGING PASSWORDS

by Jeff Bohr

Do you remember you when could use the same password for everything?

Now, passwords are likely the bane of your existence.

The worldview of password methodology. Some of the password and security breaches that have been revealed in the past few years have affected large entities like Facebook, Target, LinkedIn, Google, Yahoo! and Twitter to name just a few. You have likely had to change a few passwords in the past few years.

There are two basic rules for password management in today's world.

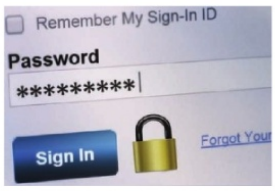
1. The password must be complex and difficult to guess.
2. The password must be easily remembered.

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 anniversaries and 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 'Amaz0n1234')

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, such as your email and online banking accounts. Re-using passwords is risky. If someone figures out your password for one account, that person could potentially gain access to your email, address, and other passwords. Your email accounts should also have a unique password as if a hacker gets access to this, they can use it to reset your passwords from your other accounts.

A great alternative to using a traditional password is to use a passphrase. A passphrase is a sequence of words strung together to create a more secure 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 three or four short words, put together in a way that does not make sense and separated by a space or symbol. If you are having trouble, walk around your house and pick a random item from each room and put them together with some random words. While this passphrase may be longer (which makes it more secure), it will be easier for you to remember. Here are some examples:

painting-platypus-incubus
tongs.decor.laptop
pillow,yearn,canonize

A passphrase should not necessarily meet all of the requirements of traditional passwords. You should choose a phrase that you can record securely, it is impossible for a human to remember all of this anymore; and to increase security avoid common phrases, lyrics, titles, and quotations. Use two-factor authentication for added security

Now, if you're like me and have dozens of accounts online, even using this system can be too much. That's how a password manager like 1Password can be a great help. It keeps your passwords secure, and you only need to remember one password to access them all. Plus, it's easy to sync with your devices via an ultra- secure web service. 1Password also has a great random password generator that will both 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.

Passwords don't need to be a cause of misery if you devise a good plan to manage them!