Why you should be using a password manager (and why your browser's memory isn't enough).

Elise Blasingame, Director of Community Education

How many accounts do you have online? Probably more than you think. With social media, online banking, email and retail sites, the accounts add up quickly. And each account calls for a new login ID and password. Ideally, each time you set up a new account, you create a unique, difficult to guess, password that does not use any personal information such as birthdates, significant others, or family member names. Every time you go online, you are likely trying to remember several different passwords at once. I have roughly 60 online accounts, and that probably doesn't include ones I created years ago and have since forgotten.

This article explores simple ways to guard these accounts in the face of hackers and the data leaks that have become more common.

Why can't my browser just save my passwords?

Many people use their browser (Mozilla Firefox, Google Chrome, Internet Explorer, Safari) to save their passwords for pages they use frequently. Ever notice how some online banking sites won't let you save your login information? There's a reason for that. If there's even a slight chance that someone might be able to access your computer, it is very easy to look up your login information in the browser's history. These 'auto-fill' features may seem convenient, but they are not secure because none of your passwords or user IDs are encrypted.

Two-step authentication

Some online accounts offer two-step verification, such as Google, Apple and now Dropbox—thanks to their recent data breach. The idea is that for an identify thief to access your account, they would have to know your username, password and get a hold of your phone. Each time you approve a specific device to access the account, such as your work computer, they will text you a code to verify that you are the one requesting access and not some hacker. It's easy, quick, and can be the difference between secure browsing and having your personal information splattered all over the Internet.

Why use a password manager?

A password manager is an application that saves all of your unique account passwords in one place and encrypts them locally so that the password manager server never even sees your password. LastPass, a popular password manager puts it this way: "We've implemented AES 256-bit encryption with routinely-increased PBKDF2 iterations." Sounds nice, right? It basically means they have a very high-level of encryption to keep passwords secure. There are many options that have high safety ratings. You can check out PCMag's article comparing popular password managers. Want even more protection? Many password managers offer the option for two-step authentication. So, you just need to remember one really strong password to enjoy the vast resources of the Internet safely.

But what if all of my passwords are the same? Or a variation of the same password that is easy to remember?

Change them all. Right now.

For every account you have online, you should have a unique, hard to guess password. Once a hacker gets one password and a user ID, they can usually access more of your accounts. When the Gawker Media Empire was hacked, millions of user names and passwords were leaked and posted online. That leak also resulted in millions of compromised Twitter accounts (the logins were the same)!

Large-scale data leaks have shown us that most people tend to use very easy to remember passwords that are too common to be safe. Passwords like *123456* are the most popular. Remember, random = safe. A combination of at least 8 characters, upper and lower-case symbols, and numbers that do not form any words is your best bet. Feeling uncreative? Try a password generator from a secure site, like Norton (they are the anti-virus people). Some password managers have a generator feature as well.

Want more? Try a YubiKey. For $25 dollars, you can purchase a thumb-drive that will essentially set a unique password every time you try to access your password manager. You can also make your own by using a thumb drive and a free software application that encrypts passwords.

This article was brought to you as part of Cyber Safety Awareness Month. Protect your privacy online, every time you log-on.