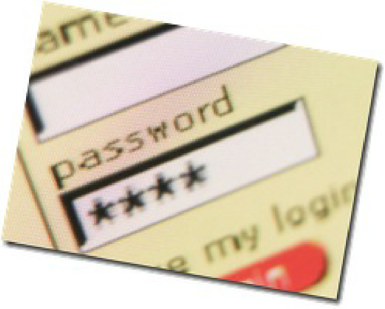
Password Tips: An Easy Way to Use Dynamic Passwords For Online Security

Alan Murphy, 2009-16-07

With all the talk going around today about the stolen Twitter documents, security of personal accounts, and password strength, there have been quite a few posts from well-wishing security folks on how to keep yourself and your online data secure. One of the *Good Idea(TM)* posts was by Seth Simonds titled "5 Keys To Keeping Personal Information Safe Online." The majority of Seth's tips are about password security and how to use unique and unidentifiable passwords for your various online destinations.



Although the gist of his post is excellent, I'm not sure I 100% agree with his suggestions on using random, nonsensical text strings for either passwords or security questions. There are few rules that people follow when passwords are concerned:

- People tend to choose easy to remember passwords because it's not something we're used to (in the grand DNA scheme of things). Sure, we can remember our PIN for our debit card without a problem, but that's only a 1:1 relationship, typically doesn't change over time (sometimes over our entire lives), and is only 4 numbers. For a fun experiment: poll your friends by asking them when they last changed their ATM PIN. When forced to remember N:N:N website:username:password combinations, we default to easy and either re-use passwords or we go with something extremely easy to guess, such as DogsName2007.
- Seth's comment to counter this is to go to the extreme opposite: create passwords that are unique to every site and are completely random, then write them down. This is almost as bad. Any password that's so hard we have to write it down to remember will never be remembered without that sheet of paper. Consequently that paper will become commonplace around our workstation. It will be left out on our desk for visitors to see; it will be kept in our laptop bags for when we're traveling; it will get thrown in the trash by mistake and then we have to start all over with 20 different websites and a new piece of paper. If something is too hard to remember then it will never be remembered; security that's too hard isn't good security.

But thankfully there's middle ground between too easy and too difficult, one that works extremely well once it's put into practice (and I'll even thrown in a twist at the end for those feeling adventurous ;). In the spirit of sharing security tips on a day when it's all over the news, here are my tips for creating and using both secure and easily recalled passwords without making them easy to guess. It's three easy steps to create almost random passwords (at least random if you don't know the pattern) that are unique to you and unique to every site you visit:

1. Choose a random two syllable compound word that has nothing to do with you personally. Let's use 'hotdog' for this example. We'll call this root word.
2. Grab the name of the website that's asking you to create a password. You can either use the entire site name if you want a long password or you can use an abbreviated version. Our example will be 'Amazon.'
3. Use numeral substitution for the website letters, changing 'Amazon' to '4m4z0n'. This is the only tricky part of the 3-step system if you're not used to it, but after a while it becomes second nature.

Now concatenate steps 1 and 3 by appending the numeric website word to your root word to create a unique password for every site that requires login credentials. Here's a list of example sites using the above system:

- Amazon: hotdog4m4z0n
- GMail: hotdoggm41l
- Technorati: hotdogt3chn0r4t1
- BestBuy: hotdog835t8uy
- Yahoo: hotdogy4h00

So on and so forth, and that's it. This nice thing about this system is that it gives you flexibility to use unique passwords for every site, be able to remember them, and keep things secure by changing your root word as frequently as you would like. Next month your Amazon password can change from 'hotdog4m4z0n' to 'dogsled4m4z0n'. The second part of the password never changes and is unique to each site; you only have to remember the root word. This system will also typically result in passwords >8 characters and includes letters and numbers, two key factors in good passwords.

And the twist? Use mixed case for your two syllable word: hotdog becomes HotDog. This is why a two syllable compound base word works so well for this system, the first character of each word can be capitalized.

This password system will allow you to use relatively strong passwords that are unique to every site without requiring pen, paper, or the memory capacity of an elephant.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com