Choosing a Strong Password

A How-To Guide by PmD Interactive

Heartbleed Was a Wakeup Call

The Heartbleed bug, announced on April 7, 2014, was a wakeup call to the World Wide Web. That which we thought was secure, really wasn't.

In this guide we'll help you choose a good password to keep you safe online.

While no one method is 100% secure, a good starting point is having a strong password.

The Length Approach

The Seed Approach

Credits

The Length Approach

You can stay safer online by following the *Length* approach to password creation.

This method relies on longer passwords that are harder to crack.

Make it hard to guess

Computers are great at doing repetitive tasks, such as guessing passwords. A computer can be programmed to try many combinations of letter and numbers at a time.

Make your password hard to crack by making it longer. A longer password keeps your private data safer from prying eyes.

- Bad: *password*
- Good: *thisismypassword*
- Better: *this is my uncrackable password*

Make it easy to remember

We must balance security with convenience: A more secure password is less convenient to remember and use; a more convenient password is less secure.

Using text that only you are knowledgeable about creates a stronger password. Text that is commonly known about you, or can be found online easily, makes for a weaker password.

- Bad: *ilikeanime*
- Good: *individualeleven*
- Better: *gits individual eleven kusanagi*

Make use of more symbols

As computers become faster and more powerful, they are able to process hundreds of thousands of password combinations *per second*.

Simply adding some capital letters, numbers, and symbols to a password makes them stronger.

○ Bad:	*mystrongpassword*
○ Good:	*MyStrongPassword*
○ Better:	*M@Str0ng_Password!*

The Seed Approach

Another method for creating a strong password is the *Seed* approach.

This method recommends you create a different password for each of your sites.

Lay the *base*

In order to use a different password for each site, we use a base to add length to the password overall.

Choose an element that does not change from site to site. This helps you remember longer passwords.

- Good: *red* + the seed
- Better: *blue* + the seed
- Best: *green* + the seed

Add the seed

To your base, you will add a seed that changes from site to site. This easily creates a new password for each site.

Let’s say, that for each site, you count the number of letters in the URL, and add it (as a word) to the base of your password. E.g. www.walmart.com

- Good: *greensev*
- Better: *greenseven*
- Best: *greenthirteen*

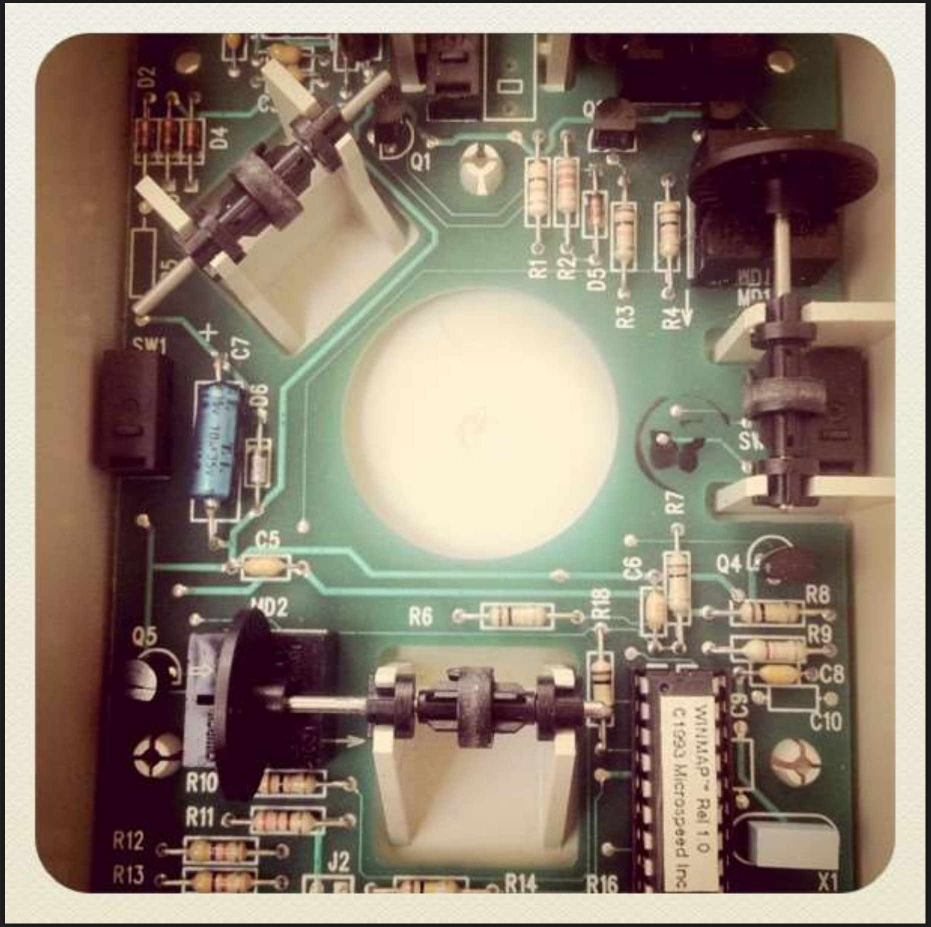
Water with *symbols*

The trick is to make a long, difficult-to-crack password, but one that has meaning to you and can be recalled easily every time you need it.

Take the previous two tips and then add a mix of capital letters, numbers and symbols.

- Good: *Greenthirteen!*
- Better: Green_Thirteen!
- Best: *Green_Thirteen13!*

Staying Safe Online is Easier Than You Think



In Short:

- A longer password is stronger
- Use words only you know
- Use a mix of letters, numbers, and symbols
- Pick a different password for each site
- No one method is 100% safe

Credits

Reference Sites

- http://en.wikipedia.org/wiki/Heartbleed
- http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/
- http://PmDInteractive.com