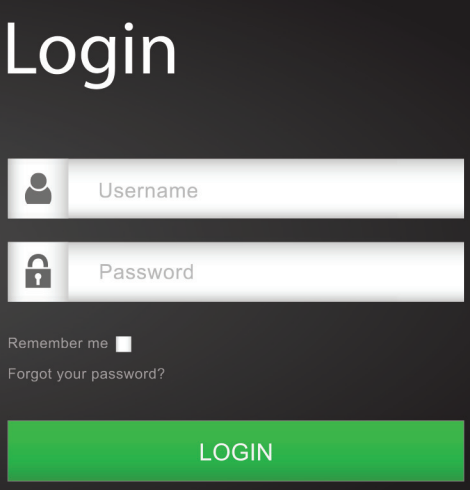
DIY: How to Develop Hacker-proof Passwords



By: David Baker

With all the publicity about cyber fraud, many people are rethinking their online security and trying to come up with hacker-proof passwords. But is there really such a thing as "hacker-proof"? At the very least, you can lengthen the odds that anyone would get access to your email, your bank account, your credit card information and your online business accounts. Here's how.

HOW PASSWORDS ARE STORED

Your bank, your credit card company, and the other sites you use don't actually know your password. They don't even want to know your password. What they store in their database is something called a "hash," which is essentially your password's digital thumbprint. When you set up an online account, the server takes your password and runs it through what's called a "hash algorithm." The result looks something like this:

5f4dcc3b5aa765d61d8327deb882cf99

It's this gobbledygook—and not the password itself—that gets stored in the server's database. When you log in, the server hashes the password you enter and compares that to the hash stored in its database. If the hashes match, they know you've entered the correct password.

Hash algorithms aren't secret, however. In fact, they're well known. Though it would take millions of years for hackers to calculate all possible hashes for all possible passwords, they've already done this for the obvious ones. So if you really want your accounts to be compromised, your best bet is to use an obvious password.

HOW TO CREATE BAD PASSWORDS

Just for fun, let's assume that you want your important online accounts to be compromised. Here are some of the most effective passwords to accomplish this goal:

- *The name of any person, real or fictional, living or dead*
- *The name of any place, such as the city or state you live in or the street where you live*
- *Any word in any dictionary, in any language*
- *A common phrase like "iloveyou" or "letmein"*
- *Any of the above, with common character substitutions (@ for A, zero for O, etc.)*
- *Repeated characters or well-known patterns ("aaaaaaaaaa" or "1234567890")*
- *Any of the above, with the letters reversed*

If you use any of the strategies above, it's just about guaranteed that anyone who wants to rip you off can do so at any time. On the other hand, if you want to create hacker-proof passwords, read on for some good strategies.

Armor Title Company, LLC
111 Dr. Michael DeBakey Drive
Lake Charles, LA 70601
O: 337-602-6351
www.armortitle.com

ARMOR TITLE
Residential & Commercial Title and Closing Services

DIY: How to Develop Hacker-proof Passwords

LOGIN

BEST PRACTICES FOR THE BEST PASSWORDS

There are two basic rules regarding bulletproof passwords:

1. The longer and the more random, the better.

2. A different password for every account or website.

Many people will see this and think, "There's no possible way that I can remember a separate super-long password for every website or account I use!" That's true. The trick is creating a formula that allows you to combine a few password components in a way you can remember. If you can recall the pieces and the pattern, you can create long, unique passwords and keep both personal and client information safe.

HERE ARE SOME BUILDING BLOCKS YOU MIGHT CONSIDER:

Pick a base that you won't forget. [BASE]

This is what, a few years ago, many people would consider a "password." It should be a moderately long word, or perhaps an amalgamation of a couple of different words. By themselves, "Rocinante" or "ChickenFeet" would be terrible passwords, but we're just getting started.

Use words that change with the times. [TIMEWORD]

Security experts suggest changing passwords every couple of months. What if you chose a different 10-letter word for each quarter of the year? For example, you could use "squeezable" from January to March, then switch to "unmuzzling" for April through June, leaving "skyjacking" and "complexify" for the third and fourth quarters.

Use some letters from the name of the website or service. [URLSNIPPET]

Though it's never a good idea to use a website URL as your entire password, you can use some letters from a website as a way to make each of your passwords unique to each site. You might take the first five letters, the consonants and then the vowels, or something similar. Whatever strategy you choose, just make sure it will work both for long and short domains.

Throw in a random number that you won't forget. [RANDNUM]

By itself, a number or date makes a lousy password. But a memorable number can be a great addition to a password algorithm. You might choose 1989 (the year the Berlin Wall fell) or 753BC (the year Rome was founded) or perhaps 1905 (the year Einstein published his special theory of relativity). Just make sure it's a number you won't forget.

Glue the elements together in a way you'll remember.

Note that you don't have to use all of the strategies above. But let's assume that you wanted to. There are lots of ways we could put together the elements of your password:

- *[BASE] + [TIMEWORD] + [URLSNIPPET] + [RANDNUM]*
- *[TIMEWORD] + [BASE] + [RANDNUM] + [URLSNIPPET]*
- *[RANDNUM] + [URLSNIPPET] + [BASE] + [TIMEWORD]*
- *[URLSNIPPET] + [BASE] + [TIMEWORD] + [RANDNUM]*

Say you're using "Snuffleupagus" as your base, "unmuzzling" as your time word and "1776" for your random number. Then suppose that your "URL snippet" strategy involves taking the whole domain of the URL and putting the first letter (capitalized) at the end. Assuming you're using the first algorithm above and this password is for your PayPal account, you'd end up with the following:

SnuffleupagusunmuzzlingaypalP1776

Now you might be thinking, "Whoa—33 characters is a lot!" That's true, but you only have to remember four things. By combining them you're able to have a unique password for every single site you use.

According to the website ***howsecureismypassword.net***, it would take a desktop computer a *tredecillion* years to crack the password above. (That's a 1 followed by 42 zeroes). Add an exclamation point on the end and a hacker would need 109 quattuordecillion years to get in. Since both of these numbers are way more than a trillion trillion times the age of the known universe, you can be pretty certain that your PayPal account is pretty safe.

American Land Title Association
Protecting the American Dream Since 1907

ARMOR A TITLE
Residential & Commercial Title and Closing Services

AN INDEPENDENT POLICY-ISSUING AGENT OF FIRST AMERICAN TITLE INSURANCE COMPANY