

How I'd Hack Your Weak Passwords

If you invited me to try and [crack your password](#), you know the one that you use over and over for like every web page you visit, how many guesses would it take before I got it?

Let's see... here is my top 10 list. I can obtain most of this information much [easier than you think](#), then I might just be able to get into your e-mail, computer, or online banking. After all, if I get into one I'll probably get into all of them.

- 1 Your partner, child, or pet's name, possibly followed by a 0 or 1 (because they're always making you use a number, aren't they?)
- 2 The last 4 digits of your social security number.
- 3 123 or 1234 or 123456.
- 4 "password"
- 5 Your city, or college, football team name.
- 6 Date of birth - yours, your partner's or your child's.
- 7 "god"
- 8 "letmein"
- 9 "money"
- 10 "love"

Statistically speaking that should probably cover about 20% of you. But don't worry. If I didn't get it yet it will probably only take a few more minutes before I do...

Hackers, and I'm not talking about the ethical kind, have developed a whole range of tools to get at your personal data. And the main impediment standing between your information remaining safe, or leaking out, **is the password you choose**. (Ironically, the best protection people have is usually the one they take least seriously.)

One of the simplest ways to gain access to your information is through the use of a [Brute Force Attack](#). This is accomplished when a hacker uses a specially written piece of software to attempt to log into a site using your credentials. [Insecure.org](#) has a list of the Top 10 FREE Password Crackers [right here](#).

So, how would one use this process to actually breach your personal security? Simple. Follow my logic:

- You probably use the same password for lots of stuff right?
- Some sites you access such as your Bank or work VPN probably have pretty decent security, so I'm not going to attack them.
- However, other sites like the Hallmark e-mail greeting cards site, an [online forum](#) you frequent, or an e-commerce site you've shopped at might not be as well prepared. So those are the ones I'd work on.
- So, all we have to do now is unleash [Brutus](#), [wwwhack](#), or [THC Hydra](#) on their server with instructions to try say 10,000 (or 100,000 - whatever makes you happy) different usernames and passwords as fast as possible.
- Once we've got several login+password pairings we can then go back and test them on targeted sites.
- But wait... How do I know which bank you use and what your login ID is for the sites you frequent? All those cookies are simply stored, unencrypted and nicely named, in your Web browser's cache. (Read [this post](#) to remedy that problem.)

And how fast [could this be done](#)? Well, that depends on three main things, the length and complexity of your password, the speed of the hacker's computer, and the speed of

the hacker's Internet connection.

Assuming the hacker has a reasonably fast connection and PC here is an estimate of the amount of time it would take to generate every possible combination of passwords for a given number of characters. After generating the list it's just a matter of time before the computer runs through all the possibilities - or gets shut down trying.

Pay particular attention to the difference between using only lowercase characters and using all possible characters (uppercase, lowercase, and special characters - like @#\$%^&*). Adding just one capital letter and one asterisk would change the processing time for an 8 character password from 2.4 days to 2.1 centuries.

Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Remember, these are just for an average computer, and these assume you aren't using *any word in the dictionary*. If Google put their computer to work on it they'd finish about 1,000 times faster.

Now, I could go on for hours and hours more about all sorts of ways to compromise your security and generally make your life miserable - but 95% of those methods begin with *compromising your weak password*. So, why not just protect yourself from the start and sleep better at night?

Believe me, I understand the need to choose passwords that are memorable. But if you're going to do that how about using something that no one is ever going to guess AND doesn't contain any common word or phrase in it.

Here are some password tips:

- 1 Randomly substitute numbers for letters that look similar. The letter 'o' becomes the number '0', or even better an '@' or '*'. (i.e. - m0d3ltf0rd... like modelTford)
- 2 Randomly throw in capital letters (i.e. - Mod3lTf0rd)
- 3 Think of something you were attached to when you were younger, but DON'T CHOOSE A PERSON'S NAME! Every name plus every word in the dictionary will fail under a simple brute force attack.
- 4 Maybe a place you loved, or a specific car, an attraction from a vacation, or a favorite restaurant?
- 5 You really need to have different username / password combinations for everything. Remember, the technique is to break into anything you access just to figure out your standard password, then compromise everything else. This doesn't work if you don't use the same password everywhere.
- 6 Since it can be difficult to remember a ton of passwords, I recommend using

[Roboform](#). It will store all of your passwords in an encrypted format and allow you to use just one master password to access all of them. It will also automatically fill in forms on Web pages, and you can even get versions that allow you to take your password list with you on your PDA, phone or a USB key. If you'd like to download it without having to navigate their web site here is the [direct download link](#).

- 7 Once you've thought of a password, try Microsoft's [password strength tester](#) to find out how secure it is.

Another thing to keep in mind is that some of the passwords you think matter least **actually matter most**. For example, some people think that the password to their e-mail box isn't important because "I don't get anything sensitive there." Well, that e-mail box is probably connected to your online banking account. If I can compromise it then I can log into the Bank's Web site and tell it I've forgotten my password to have it e-mailed to me. Now, what were you saying about it not being important?

Often times people also reason that all of their passwords and logins are stored on their computer at home, which is save behind a router or firewall device. Of course, they've never bothered to change the default password on that device, so someone could drive up and park near the house, use a laptop to breach the wireless network and then try passwords from [this list](#) until they gain control of your network - after which time they will own you!

Now I realize that every day we encounter people who over-exaggerate points in order to move us to action, but trust me this is not one of those times. There are 50 other ways you can be compromised and punished for using weak passwords that I haven't even mentioned.

I also realize that most people just don't care about all this until it's too late and they've learned a very hard lesson. But why don't you do me, and yourself, a favor and take a little action to strengthen your passwords and let me know that all the time I spent on this article wasn't completely in vain.

Please, be safe. It's a jungle out there.