Advice from a Real Hacker How to Create Stronger Passwords

By **occupytheweb** 04/19/2018 2:13 am

People who know that I am a professional hacker often ask me what they can do to make their computers and personal information safe from people like me. The answer, of course, is that nothing will make you completely safe, but there are a number of measures any computer user can take to reduce the chances of being a victim of a hacker.

Don't Miss: Diceware Gives You Truly Random yet Easy-to-Memorize Passwords

Why You Should Be Choosing Stronger Passwords

As your password secures all of the resources on your system, including your email and other important online accounts (banking, brokerage, etc.), it's critical to choose a strong password that makes my job more difficult. Understand that there is NO password that I can't break given enough time and CPU cycles, but like anything else, I'll attack the low-hanging fruit first.

Image via Shutterstock

Let's begin by saying that hackers like me don't simply try to guess your password at your login screen. That would be impractical. Most login screens lock an attacker out after three incorrect attempts. I want to be able to try millions or billions of attempts.

What attackers will do is steal the **storage** of the passwords on a vulnerable system. These passwords are encrypted in the form of a hash, but once I have these hashes, which I can grab using tools like Pwdump, Airodump-Ng and the Meterpreter, I can take as much time as I need to crack your password.

The Best Way to Make Your Password Less Appetizing

Ideally, you should choose a random set of characters that is the maximum length that your account or system will accept. The fundamental rule of password cracking is that the longer the password, the longer is takes to crack. Then, change the password often, about every thirty days or so.

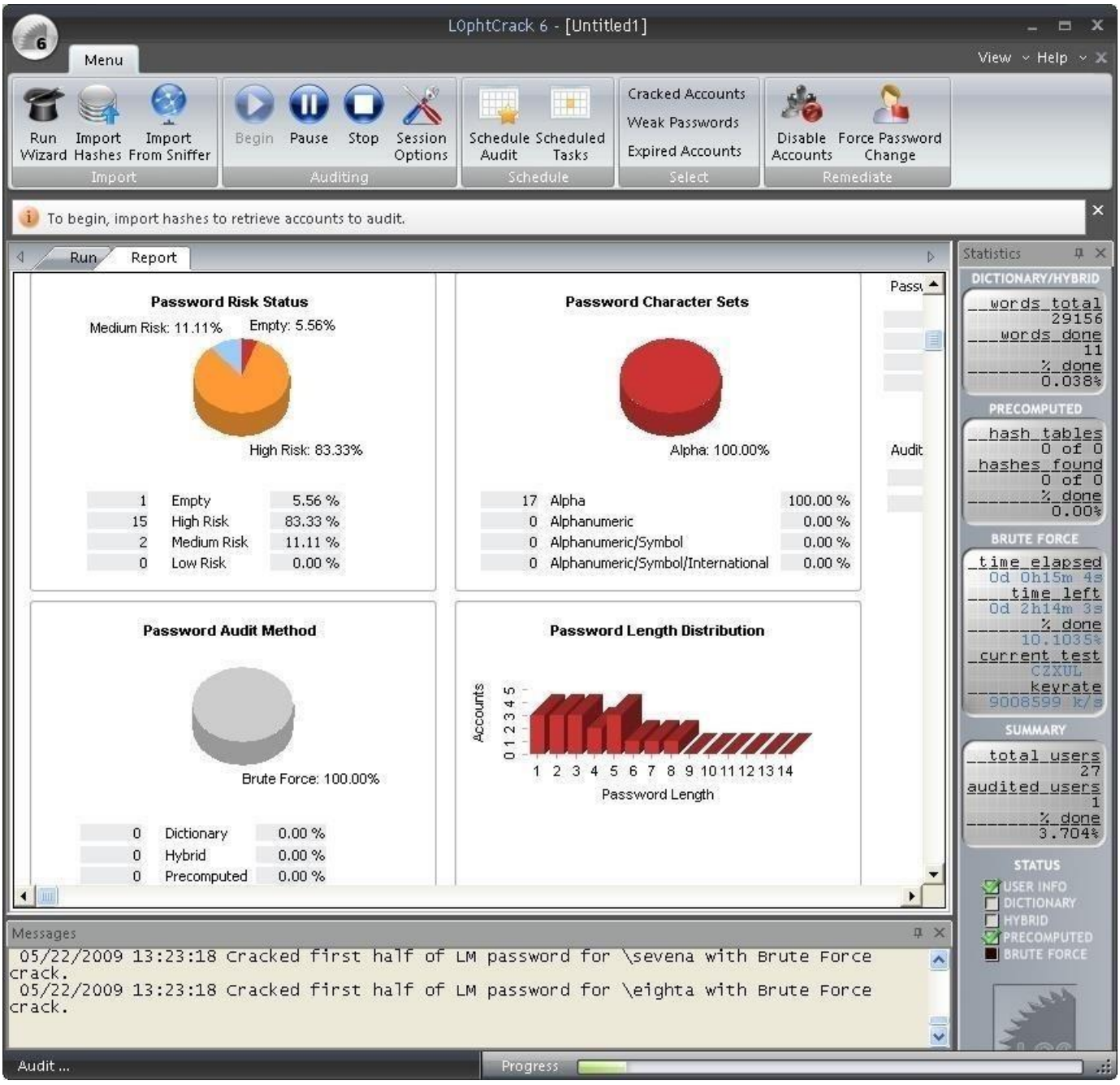
I think it goes without saying that this ideal scenario is not a realistic scenario for most people. Given that, let's look at how you can better protect your system and accounts from hackers like me. Here is some advice on how to make my job as difficult as possible, while remaining practical.

Step 1 Never Use Dictionary Words

Even a hacker with a minimal skill set can easily crack passwords that are found in the dictionary. You might think that your word or words are rather unique and obscure, but it doesn't take me very long to test every word and word combination in the dictionary. NEVER use a dictionary word!

Image via Shutterstock

Even if you add numbers and special characters, hacking tools like Crunch will let me create custom wordlists, and tools like Hashcat, Brutus, Cain and Abel, THC Hydra, John the Ripper, Ophcrack, and L0phtCrack, as well as Aircrack-Ng and Cowpatty for Wi-Fi, will help me crack the password using my wordlists.

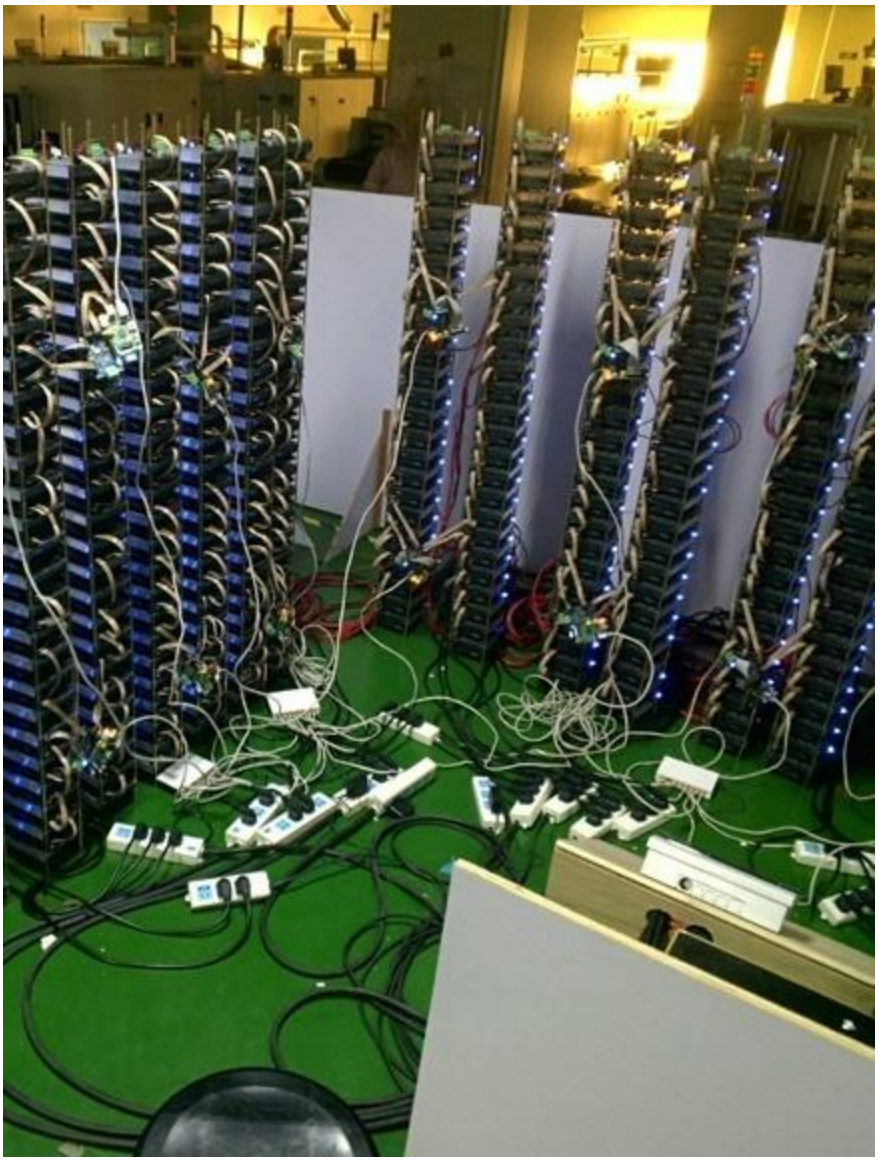


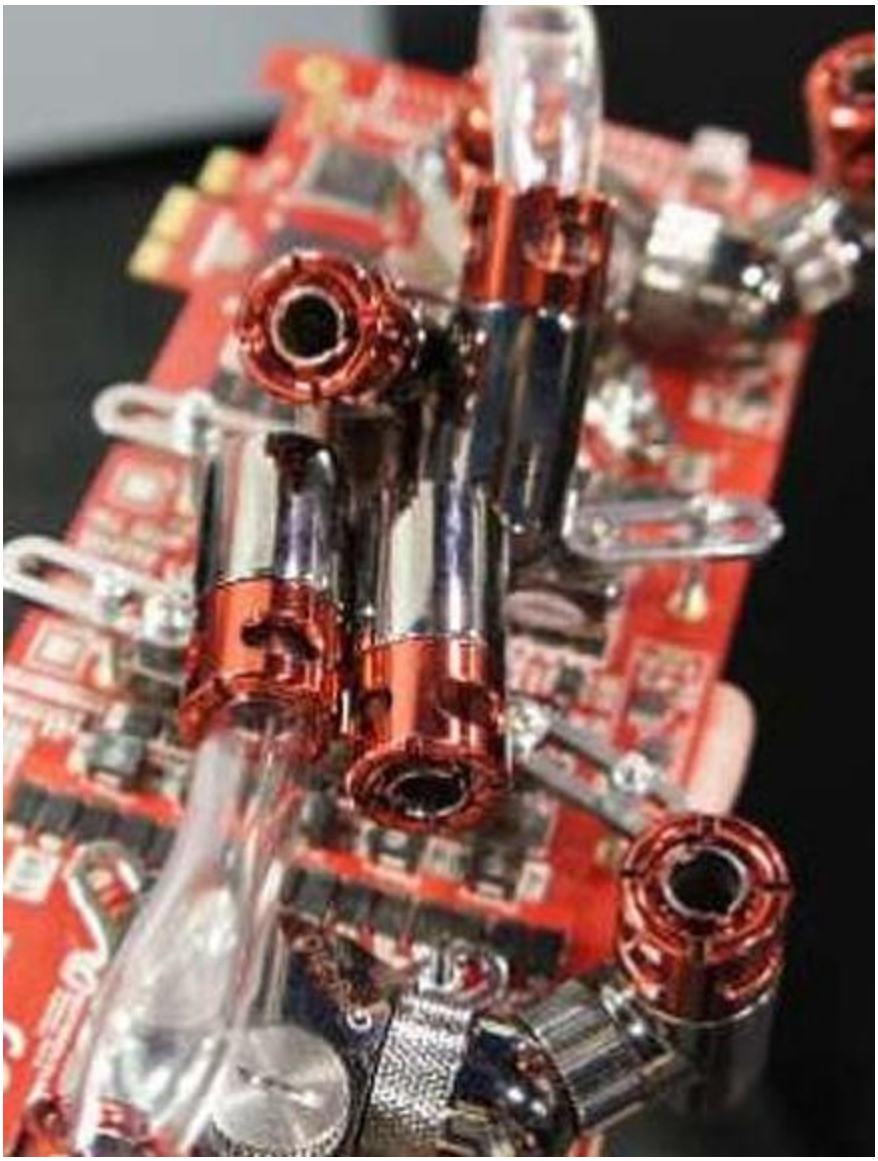
Using L0phtCrack to crack passwords. *Image via [L0phtcrack]*

Step 2 Use All of the Allowable Character Types

Password cracking that tries all possibilities is called [brute-force password cracking]. It simply tries every possible combination of characters until it finds your particular password.

It can require much time and computing resources to do so, but with recent developments in parallel processing, specialized password-cracking ASICs, and the use of botnets and GPUs, brute-force password cracking has made some giant leaps toward making even long, complex passwords more feasible to crack.





(1) Bitfury boards by Black Arrow, (2) Butterfly Labs processor, (3) Inside the Butterfly Labs Monarch. *Images via Bitcoin Talk, CoinDesk, Gizmodo*

As you might guess, brute-force password cracking is capable of eventually cracking any and all passwords, but the keyword here is "eventually." To protect yourself, you want to force the hacker to take long enough that they will give up and crack your colleague's or neighbor's easier password before they crack yours.

To slow the hacker down, make certain that use at least one of every character type in creating your password. This means using at least one lowercase, one uppercase, one number, and one special character. This will force the hacker to include all of these characters into their brute-force cracking character set, thereby forcing them to take much, much longer to crack your password.

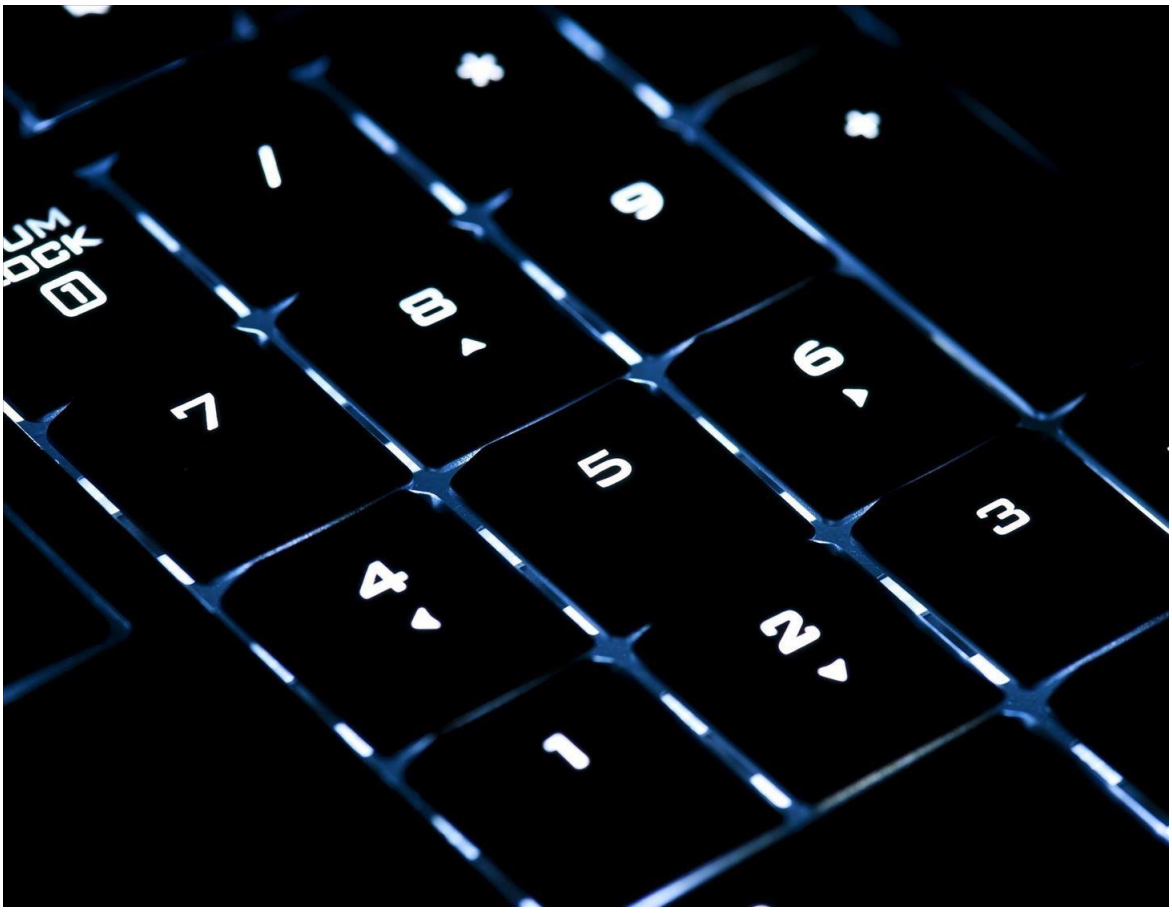
To demonstrate, the amount of combinations that are possible with an all lowercase, 8-character password is 26 raised to the 8th power, or 208 billion. Albeit, that is a big number, but it is certainly possible for the hacker to run through that many possibilities in short order.

If you use lowercase, uppercase, digits (0-9), and special characters, the number of possibilities that the hacker must try is 75 raised to the 8th power, or 1,001,129,150,390,625. That's 1 quadrillion possibilities! This translates into about 5,000-fold increase in the number of possibilities the hacker must try.

To think of it another way, if the first password (8 characters, all lowercase) took 1 hour to crack, the second one would take 5,000 hours, or 208 days. That may be enough to frustrate the hacker.

Step 3 Never Use Just Numbers

NEVER use a numeric password without any letters or special characters. You are making things way too easy for me!



Never just use your number pad. NEVER. *Image via Shutterstock*

Since there are only 10 digits (0–9) in our base 10 number system, even a numbered password with 10 characters only amounts to 10 billion possibilities to brute-force. Compare that to an eight-character all lowercase password with 208 billion combinations, and it would be 20 times easier to crack your 10-digit numerical password than the 8-character lowercase one.

That's simply child's play! Give me more of a challenge than that!

Step 4 Change Your Password Often

It's important to change your password often. "Often" is a relative term and it will depend upon the value of the information being secured by the password. If it is an email or online bank account, you might want to change your password every three months. Other passwords, such as your accounts on non-financial websites, once every six months or year is probably sufficient.

The reason you need to change your passwords periodically is that hackers like me are always gathering passwords from accounts all over the world. We may not use them immediately, or we may sell them to someone who hasn't done anything with it yet. Your password may be compromised and you don't even know it yet.

By changing it periodically, you significantly reduce the chances of someone like me compromising your account, even if the website/domain has been hacked.

Step 5 Use Different Passwords on Different Accounts

Your passwords are stored all over the world in various accounts, websites, domains, etc. If you use the same password on all of your accounts, your information is only as secure as the weakest system storing your password.

Imagine a case where you find a website or a game online that you think is fun and entertaining. They ask you to create an account and a password. This might be a new company or a big company, but if they don't secure their systems adequately, someone will hack their system and steal yours and all of the other accounts' passwords.

As a hacker, I may not have any interest in your account on that website, but I will try it on your bank account, credit card account, email account, brokerage account, and so forth. If they are all the same, I have struck GOLD!

The rule here is to use different passwords on different types of accounts. You might create one password for all of your highly confidential accounts, and one password for all the other accounts. That way, if that online game site gets hacked, I can't take that password and get into your bank account.

Step 6 Create a Passphrase

Probably, the method that will frustrate hackers like me the most, is to develop a passphrase that is long and includes no words and all of the available character types.

I have seen many articles online that advise folks on how to create passphrases and I simply laugh at them because I know that their advice will simply create a passphrase that is still easy for me to crack. Things like adding a date and month after a word, reversing the order of dictionary words, and so on just beg to be cracked in short order.

Here is what will make my job most difficult.

First, create a phrase or sentence that is meaningful to you. In this way, it will be easy to remember. For instance, "I love mountain biking and hiking." Now, take that phrase and convert it into single string of uppercase, lowercase, numbers, and special characters, like this one:

"I<3mtnb1K1ng&H1k1ng" may not be an impossible passphrase to crack, but it's definitely harder. *Image via Shutterstock*

Note that I have converted "love" to **<3**, "mountain" to **mtn**, "biking" to **b1K1ng**, "and" to **&**, and finally, "hiking" to **H1k1ng**. It is critical to intersperse special characters and numbers into the passphrase as well as use both upper- and lowercase letters.

This creates an 18-character passphrase that uses uppercase, lowercase, special characters, and numbers that, although not unbreakable, would make someone like me invest significant time and computing resources to crack it.

Most importantly, because it has special significance to you, you will remember it. Obviously, this is key. No matter how complex, passwords or passphrases that you can't remember defeat the whole purpose.

That's because people often write down passwords they can't remember and hackers like me will often find your passwords on a sticky note near your desk. Usually in the top drawer, under the keyword, stuck to monitor... you get the picture.

Now, How Do You Feel About Your Passwords?

I hope this advice makes my job as difficult as possible to crack YOUR passwords, but thankfully, so many people won't take this advice that I know there will always plenty of easy pickings among your neighbors and colleagues.