Your Passwords Stink - And How to Fix Them

Author	josh
Date	2021-01-17 13:48:06

Overview

For better or for worse, passwords are at the center of how we secure our digital lives. For your phone, your PC, and your likely 50+ online accounts - you have a password standing between a thief and your data. Unfortunately, most of us have been told un-truths about what makes a password secure, leaving us vulnerable to password-cracking hackers. Let's discuss how passwords are stored and cracked, what makes a password secure, and where to store your passwords safely.

Password Permutations - The Secret to Secure Passwords

Length vs. Complexity

Most of use have been told, frankly, a lie about what makes a password secure. It's not an intentional lie, but technology changes fast and the conventional wisdom around password security is very outdated. Most of us have been told that a password like this is pretty secure: **B@nk1nG**. But which is more secure? **B@nk1nG**, or **MyMoneyAccountHere**? It turns out that the latter (MyMoney...) is much more secure than the word banking with a bunch of symbols changed around.

Length matters much more than complexity for password security. But why?

How Passwords are Stored and Cracked

To understand why this is important, we need to understand how passwords are stored and how they are cracked by hackers. When you visit your Gmail account, Google does not store a plaintext copy of your password "MyPass". Instead, they store what is called a *hash* of the password. The hash is a one-way function that turns some data into a signature, and does so in a way that the same input always gives the same output!

So let's say Google stores the hash "fb3f06c82…" (MD5 - old and outdated hash that isn't used anymore). When you visit Google.com, you type in "MyPass". On the Google server, they run MyPass through the hash function and compare the hash to the hash they have stored in their database. If they match, you are allowed in!

What happens when hackers compromise a websites password database? They don't get a giant table of passwords, they get *password hashes*. And since a hash is not reversible, they have to *guess* a bunch of possible passwords until they find a matching hash! The naive way of doing this is called *brute-force* - you guess every possible combination of characters until you find one that matches the hash you are looking for.

Now, brute-force is not the only way to guess passwords. Attackers also use sophisticated techniques like *dictionary attacks* that look for commonly used words and passwords. They can also pre-compute *rainbow tables* with password guesses for faster lookup than brute-force.

Back to Length vs. Complexity

Why does length matter more than complexity then? It makes the math of brute-force password guessing *much, much harder*. If you're going to brute-force a password database, you have to try a lot of possible combinations. So if you make the *total number of combinations* mathematically difficult to deal with, you make brute force a practically impossible task.

The math of password combinations is fairly simple. For a given character space (possible characters) *c* and password length *l*, the number of possible combinations is $\mathbf{c^l}$. That's *complexity, to the length power*.

For example, if we have a 4 character password of numbers, uppercase, and lowercase letters: That's 62 possible characters * 62 * 62 *62, or 62^4.

Let's look at this with some concrete examples. I've written a program calledpassperms that shows the number of possible permutations for length vs. complexity changes, with crack times for consumer and professional hardware.

If we add a bunch of characters like 1@!$ to an 8 character password, that only changes the crack time by a few *hours* on *consumer grade hardware:*

```
./passperms -c -r
 Combinations for constant length 8, variable complexity
 Cracking w/ 7.652 GH/s, MD5 - NVidia GeForce 1050 Ti consumer laptop
 Complexity           Combinations           Crack Time
   10.                   1.E+08            0.00056 seconds
   26.                   2.E+11            1.16015 seconds
   52.                   5.E+13            4.94998 minutes
   62.                   2.E+14           20.21668 minutes
   72.                   7.E+14            1.11451 hours
   82.                   2.E+15            3.15454 hours
   92.                   5.E+15            7.92004 hours
```

I don't know about you, but if my password is leaked I don't want a few hours standing between me and account compromise. I want an amount of time that is near impossible. And we can get that, by making our password *longer* instead of necessarily *more complex.*

With a 62 character space (just numbers, uppercase, lowercase letters) going from 8 to 12 characters makes the difference between *hours and* ***years*** for brute force cracking:

```
./passperms -l -r
 Combinations for constant complexity 62, variable length
```

```
Cracking w/ 7.652 GH/s, MD5 - NVidia GeForce 1050 Ti consumer laptop
Length           Combinations            Crack Time
   8.                   2.E+14            20.21668 minutes
   9.                   1.E+16            20.89057 hours
  10.                   8.E+17            53.96729 days
  12.                   3.E+21           567.96791 years
  14.                   1.E+25         2.18327E+06 years
  16.                   5.E+28         8.39248E+09 years
  20.                   7.E+35         1.24010E+17 years
```

What a difference! And that is why length matters more than complexity. You are better off with a pass*phrase* rather than a short password with a bunch of symbol substitutions.

It is also important to note that the overall *entropy* (randomness) of the password matters. I just want to hit home the general idea that a longer passphrase will serve you better than a short password with a bunch of wing-dings in it.

Bad: **B@nk1nG**
Better: **ThisWhereIKeepMyMonay**
Best: **KZEEldaGkeOnYm9H4coe**

Password Managers - the Best Practice

Now let's discuss how to safely store and even generate secure passwords! This is the practical advice section - something you can do *today* to make your passwords better.

The first thing you need to be aware of is that password *reuse* is a very, very bad practice. You're likely re-using a password on multiple sites right now, and you need to reconsider doing so. The reason is simple - if a hacker gets access to that reused password, they now have access to *multiple sites*! They could compromise a significant portion of your digital life.

Google's password database is very, very secure. But thingstore.com might not be - and if hackers compromise your reused password for thingstore.com, they now have access to your Gmail account. Best practice is to generate *unique* passphrases for each and every account you have.

But Josh, how will I remember all these passwords??? In the last section, I mention that a random, long string such as **KZEEldaGkeOnYm9H4coe** makes a great passphrase, how could one possible remember that one password let alone 100 of those???

The simple answer is, *you don't*. Instead, you use a *secure password manager program* to generate and store your passwords!

A password manager is a very secure, special piece of software that encrypts all of your passwords into a database. Instead of remembering 50 passwords, you only have to remember *one very, very good one called your "master password"*. Then, you can simply use the password manager to auto-fill passwords on websites or copy-paste them.

Two great options include the very user-friendly *LastPass* and the open source *KeePass*. There are plenty of other options as well. At the very minimum, an OpenSSL,PGP, or LibreOffice encrypted file (using AES-256 or another secure encryption algorithm) may suffice, but using a *purpose built* program will be the most secure option.

A Word About Password Manager Security

A good master passphrase is something long and memorable, unique to you. For example, *ManualTransmissionDrivingRocks*. Better yet, you could use *diceware* to make a random string like *BikeEthicsObserveMind*. You commit that one good password to memory, or even write down a backup to keep secure in your safe or safety deposit box.

You may ask, does having a password manager mean I have a single point of failure? In practice, this doesn't matter - because by using a password manager, you have significantly lowered the *attack surface* in a very significant way.

The vast majority of hacks are *broad* rather than *narrow*. In other words, most hackers are not targeting *you specifically*. Most breaches go something like this: a hacker compromises Target's password database. That database is leaked, and password crackers immediately find the crappiest passwords in the database that are also likely reused. Hackers then use that information to log into people's Gmail accounts and send out spam.

By using a password manager, you are preventing 90% of hacks from affecting you. For someone to breach your stuff, they now have to know you use a particular password manager, somehow gain access to **both** your master password (through some malware/phishing) **and** your encrypted keystore, and then get your accounts. If someone has gotten this far, you are both *already compromised in a big way* (ie: someone has access to your device) *and* are being targeted specifically.

I'm not saying this is impossible at all, but rather it means you have bigger problems. Other security mechanisms such as 2 factor authentication will also be very important to have. But by using a secure password manager, generating un-brute-forceable passwords, and avoiding password reuse, you have prevented a huge portion of broadly targeted hacks from compromising your digital life.

Secure Passwords and Password Managers

If this article hasn't already scared you into changing some bad password practices, I hope it has planted the seed in your head at least!

We've learned that short but complex passwords are the worst of both worlds - hard to remember and easy to crack. We've learned that longer pass*phrases* are a much better protection against password cracking, and randomly generated ones even better so. Just a few characters makes the difference between hours and years!

Finally, we've discussed the use of secure password managers as a best practice for securing your digital life. Time to set up a password manager for yourself and start changing those passwords! Stay safe out there.