Security Best Practices - Part 1: Passwords

Travis - 2021-03-16 - Best Security Practices

1. Passwords

TL/DR: Use a reputable password manager with 2FA (Two-Factor Authentication) and at least a 20 character password which is different on every site.

Passwords are one of the easiest (and first) ways to fail when it comes to internet security. We're always told to have a secure password but not told how to make one or why. It might shock you to know the two most common passwords are '123456' and 'password'. This is because most people forget to change from the default password supplied with their new device or system.

Password security can always be broken. Always. It simply all depends on how long and how much effort it would take. For example, most people's router username and password are still admin/password. That would take about 4 seconds to enter with next to no effort.

NIST System

A lot of websites opt for the recommended NIST system of requiring 8 characters with at least one uppercase, at least one lowercase, at least one number, and at least one special character. Using this system, it would mean a password would look something like 'Pas$w0rd'. This is still not secure. As stated earlier, passwords will always be broken. They are often broken through either guessing (social engineering), malware (keylogging), or brute force.

There are 6.63 quadrillions of different possible 8 character passwords and at the

Passwords^12 convention in 2012, Jeremi Gosney demonstrated a machine that broke all 6.63 quadrillion passwords in 5.5 hours. That equates to 350 billion password guesses per second. And this was in 2012...

Entropy

Password strength is called password entropy and entropy is based on the character set used (uppercase, lowercase, numbers, and symbols) as well as length. Password entropy predicts how hard a password is to crack using guesses, brute force methods, dictionary attacks, or other methods.

If a password uses numbers (0-9), uppercase (A-Z), lowercase (a-z), and special characters (!"£ etc), there are 95 possible choices for a one-character password. If the password is two characters long there are 9025 possible choices and for three characters there are 857375 possible choices (and so on with the equation being expressed as 95^n (with n being the number of characters in the password)).

As a species, humans make terrible choices for passwords. Even if a person chooses a 'random' password, we have a bias towards certain letters and numbers. This is called letter frequency and can easily be seen in the game Scrabble. There are more letters E (12) than Q (1). Nobody wants to get the Q or the Z. In addition, humans are notoriously bad at remembering random strings of letters and numbers, so we either write it down (which is a very bad idea for a password) or we make it easy to remember.

- "Pas$w0rd" is a bad password as it's easy to guess.
- "0il;vSHJ" is an okay password as I mashed the keyboard.

Both have the same amount of entropy but it would take less than 6 hours to guess either password with Gosney's machine. As such, neither is secure.

Securing your Password

Because you can't change the option of accepted characters, you can secure your password through the number of characters used on your password. This is where the 95^n comes in and that means 95 multiplied by itself however many characters are in your password. That means the password entropy on an (8) eight-character password is worked out by;

- 95 x 95 x 95 x 95 x 95 x 95 x 95 x 95 (and is written as 95^8)

This equates to 6.63 quadrillion different possible passwords. A more secure password would be at least 20 characters long (95^20) and would equate to 10.24 decillion possible different passwords. For reference:

- 6,630,000,000,000,000 = 6.63 Quadrillion
- 10,240,000,000,000,000,000,000,000,000,000,000 = 10.24 Decillion

Using Gosney's machine on a twenty-character password could potentially take up to

9,277,379,140 years to crack a single password...

Password Managers

Well great, it will take over 9 billion years for someone to crack my password, but my password isn't the only one out there. My password is secured by someone else and that someone else may not (probably not) be as vigilant as me and as such my password is only as secure as their password.

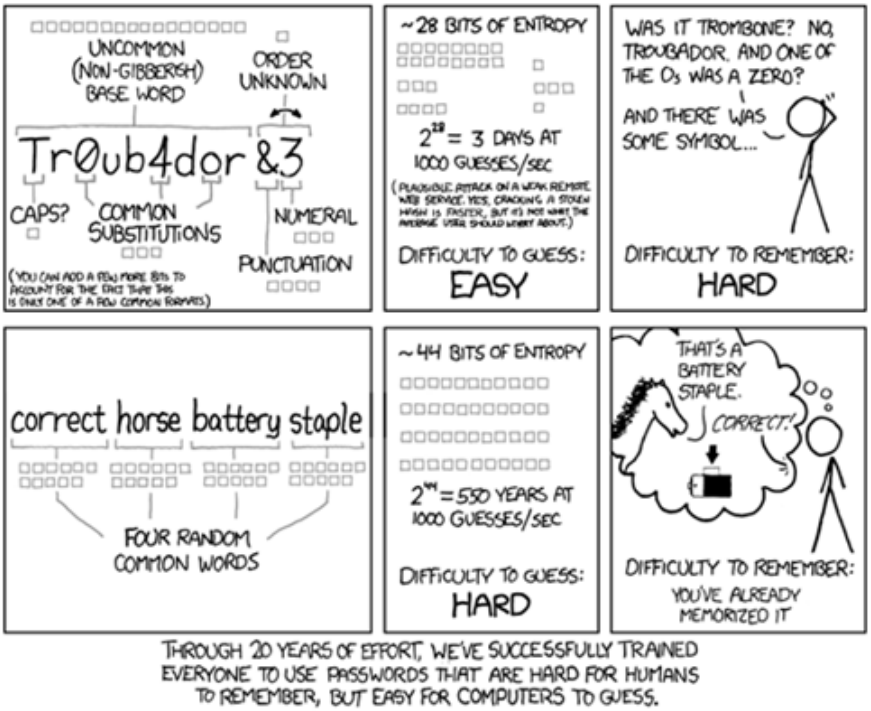
Now because my security is only as good as the weakest link in the chain, industry practice states to have a different password for every site. This is a great idea, but I doubt I can remember a single twenty-character password, let alone a different twenty-character for every single site I'm registered on.

Luckily there is software that nullifies that issue: Password Managers.

A password manager is a piece of software that stores all the secure passwords in an encrypted database that can only be accessed with the correct password (which should still be twenty characters or more). This may seem like a weak part of the plan having all the secure passwords stored in a single place secured with a single password, however, this can be further overcome with the addition of Two-Factor Authentication (2FA). This is where a hardware device is used to authenticate that you are the correct holder of the account and you're authorized to access it.

This ensures that all your passwords are secure, encrypted, and still easy for you to access. Granted even this isn't 100% secure, but it's as close as we can get.

My little trick for a completely random password that's easy to remember? Get a dictionary and open it to a random page. Close your eyes and stick your finger on the page.... closest word is chosen. Do this 4 or 5 more times. That's your password....



And because someone said it a lot better than me...

For the sake of clarity and transparency, I personally use LastPass with a Yubikey as my 2FA and if someone wants to read my email in 9 billion years, I won't exactly care...

Tags

Security

Related Content

- Are there any restrictions on what characters can be used in my password?