Passwords are keys to our digital world.

The first computer password was created by Fernando Corbato’s team for CTSS (Compatible Time-Sharing System) multiple user computer. That password was absolutely insecure.

Since a World Wide Web became available to the public, passwords were required almost for everything. Instead of remembering long strings of random letters and numbers, majority of people decided to choose an easy way by making easy and memorable passwords. They actually still do that. The top worst and insecure passwords are “password”, “123456” and other similar combinations. Millions of people seem to think “password and “123456” are secure passwords!

In 1979 was invented a Data Encryption Standard (DES is a symmetric-key algorithm) what allowed to keep passwords in an encrypted form. That standard remained for nearly 20 years, but in 1998 the Electronic Freedom Foundation broke a DES key just in 56 hours and that standard was accepted as insecure.

In 1997 was Invented an Advanced Encryption Standard what was an enormous achievement for the world of passwords as a cracking of AES key would take years to crack. The same year a CAPTCHA was introduced for additional security (a way to generate random images of text what computers were not able to read).

[Nowadays we live in a Fast-Paced Digital World](http://www.business2community.com/business-innovation/stay-relevant-todays-fast-paced-digital-world-01133550) where many new standards are released and get deprecated with a time, but none of them a 100% secure. It looks like in the future we will be using a bio keys for an authentication (our body) and a computer intelligence to help us with that.