Introduction

This article is of an informative character and is intended for secondary school students – it can be treated as a revision of issues introduced in a junior high school. Multimedia texts and materials are to encourage the recipients to use modern electronic devices and possibilities produced by the contemporary informative world in a responsible way. The main aim of the article is to persuade readers to consider problems concerning the security of passwords.

Passwords – code words were already used in the Ancient times. Earlier they were used to convey coded secret information concerning e.g. the plans of action of a neighbouring enemy. Information was provided orally or in writing. However, such a security method had a lot of disadvantages – the transferring party (e.g.: a spy) could venture selling the information at a higher price for somebody else. The situation has changed, the range of password usage has been broadened, and people responsible for their obtaining and capturing do not hide in the dark corners of the streets any more.

Why should good and strong passwords be applied?

First and foremost, in order not to lose property (e.g.: money) or due to moral damages (e.g.: losing letters from an e-mail). The latest news concerning leaks and breaking passwords shows the attitude of users to their own security – some examples of the mentioned phenomena have been presented below:

Leaks of almost 10 000 passwords from portals onet.pl, wp.pl, interia.pl, o2.pl
The list of over 3500 logins and passwords of polish e-mail accounts
The list of passwords from Gadu-Gadu + zapytaj.onet.pl
The password of the Prime Minister stuck to his laptop.
Nauki ścisłe priorytetem społeczeństwa opartego na wiedzy

Artykuły na platformę CMS

The most popular passwords in Poland

| 123123 | damian | 123456 |
| qwerty | 123456789 | 111111 |
| qwertyl | piotrek | dupa |
| marcin | marcin1 | **** |
| 1234 | asd | aaaaa |
| qazwsx | qwel123 | polska |
| mateusz | abc123 | matrix |
| 123qwe | qwert | monika |
| zaq12wsx | haslo1 | master |
| michal | haslo | myszka |
| maciek | admin123 | misiek |
| zxcvbnm | | 098765 |

Own analysis of the most popular passwords.

If our “password” is similar to those presented in the table above, we should change it immediately and think about a new one while reading the further part of the article.

How to create a perfect password?

The only limit for creation such a password is the finite number of characters on the standard keyboard which we can admire in QWERTY system. Having 95 basic characters ASCII – letters, numbers, punctuation marks and special characters (without 33 characters, so called control codes), we can without a problem create a very strong password, for instance: with the combination of $7 \times 10^{15}$ (using 8 from 95 characters) and $4 \times 10^{31}$ (using only 16-character password from the set of 95 characters).

---

1 Own analysis on the basis of the set of passwords.
2 95 characters visible on QWERTY keyboard, in reality there are much more of characters.
3 *ASCII - American Standard Code for Information Interchange*
What should be a strong password like?

- It should be possibly the longest, i.e. it should contain at least 8 characters and be comprised of the greatest number of different characters, except for letters and numbers, and special symbols should also be used: space, commas, and dashes.

- It is not advisable to use any words, names or anything which may be found in a dictionary because the attacks on the password begin with attempts to break it using dictionary methods.

- It is wrong to repeat characters or to apply the known order of characters e.g.: 12345. Such a password is broken at the very beginning, and using a similar order in a strong code weakens the password a lot.

- The password should not contain personal data such as name, surname, birthdate, family data, dog’s name – such information can be easily obtained, that means breaking the access code quickly.

- Although, the code 1337H@XXoR seems to be strong, in reality it is not. Modern password breakers are often based on replacing similar to letters characters. Thus, one should create more serious passwords.

- The same password should not be applied to all the websites/services – if an unwanted person has gained the password, they will probably get the access to our other accounts.

The strength of a password is not only conditioned by its length. A 32-character code comprised only of lowercase alphabet letters will be much weaker than the 16-character code built from capital/lowercase letters and numbers, and the best possible combination will be a code including 8 characters from all 95 basic ASCII symbols and it will be the strongest one from all the depicted below examples:

---

4Graphics QWERTY Keyboard.png
Of course a reader is much more ambitious than just to learn an 8-character password. Thus, it is time to discuss more complicated and secure access codes.

Creating a safe password

One should first consider whether the password will be created by them or if it should be done by the password generator. The password created by a human will contain certain common traits, for example capital letters at the beginning and a number at the end, it will also have references to the spoken language, where properly built programme will use these regularities to break the code. Generators are better at creating a heterogeneous password but at the same time such a password will be more difficult to remember.

If a reader decides for the password created on their own they will for sure remember it quicker because: they will be the author of the creation, they will know the origins of the password creation, they will be aware of the possible mistake (vide. weak password).

An interesting and easy to implement way will be using a chosen chant that we know. First, write it on a piece of paper or elaborate on it using any „medium“ such as: Internet, volume of poems, book, newspaper, presenter on TV, carton of milk.

For instance:

The content itself is not the most important, what is actually needed are the first letters of each word, to make it more difficult it is possible to use punctuation marks and count the number of letters in each word, add these values to our set. What will receive a reader linking the first letters of each word, punctuation marks and writing each letter alternately as lowercase and
As a result, a new, quite complicated and strong password has been formed.

I suggest practising the above method, not necessary strictly sticking to its rules. I simply encourage to think of own manners of forming a new password.

If a reader decides to form the password using an artificial method, i.e. by password generator, they can use the following websites:

1. **GRC’s Ultra High Security Password Generator**
2. **Secure Password Generator**
3. **passphra.se**

Besides the generators, there are managers for managing the password sets:

1. **KeePassX**
2. **KeePass**
3. **PINs**

**How to quickly and painlessly remember a long and complicated password?**

Use a pinch of imagination looking at the keyboard and notice for example pictures typical of African safari:
In this simple manner it is possible to put into the brain an extremely long password knowing its origins or rather the origins of the story. Has the reader suspected that they remembered such a password:

```
@Lt\D#s_3G\@=k/r<p$s%w%$s~_.
```

If the password has not been rooted in memory, it means that the story was not interesting enough, then the reader should tell his own story.

The password which is resistant to brain can be written down on a piece of paper, then it should be kept nearby and it should not be shown to other people. While using the code memory will absorb information, and fingers writing the code will soon know it better than a piece of paper which finally must experience the consequences of its dangerous knowledge.

If we do not want the rest of innocent pieces of paper share the fate of the predecessor it is possible to write down the password manifestly, so as a possible aggressor/evil buckle/cracker will not guess what is the real content of our note. It is enough to write down on a small piece of paper a logic order of characters, a strange poem, the shopping list or a letter to a sister. We can take a pricelist of a computer set with the names of subcomponents as an example.
We choose e.g.: every fifth and eleventh character of a line, repeat the proceedings till point 5.) so as the password would not be too long. Our new code has such a form:

```
aGM1ar7Mi[Szb<BTro
```

The strategy demonstrated above concerning creating a strong password is only an example which may be modified. Then, I suggest taking out the pieces of paper...and create your own method, a unique code card. You can share the ideas with others, in such a way an additional „algorithm” will be applied, and your code will be stronger.

Good luck!

**Interesting facts:**

The weakest link in a password/code is most often the human himself.

How will we probably imagine breaking a password by a cracker/institution for breaking passwords:
- Let’s use anti-cryptographic system worth 3 million PLN to break this impossible to guess password and let’s check what’s next!

How can really breaking a password look like:
- Let’s use that wrench worth 30 PLN, we will strike with it as long as they give us a password.
And remember, dear readers!

*Passwords are like underwear – Do not leave them where they can be seen. Change them regularly and do not lend them to strangers.*

**Bibliography:**


**Internet sources:**

3. Checking the password’s strength - [http://howsecureismypassword.net/](http://howsecureismypassword.net/)
Nauki ścisłe priorytetem społeczeństwa opartego na wiedzy

Artykuły na platformę CMS

5. Codes ASCII. - [http://www.asciiart.com](http://www.asciitable.com)

6. Graphics “QWERTY Keyboard.png” comes from [Wikimedia Commons](https://commons.wikimedia.org) and is on the licence [Creative Commons Attribution-ShareAlike License](https://creativecommons.org/licenses/by-sa/2.0/)

7. Sources for analyses -

8. An idea for the picture "Passwords are like underwear" has been taken from [http://churchm.ag/remind-your-ministry-about-passwords-send-them-this-image/](http://churchm.ag/remind-your-ministry-about-passwords-send-them-this-image/)