5 Tips for a Secure Password

World password day

by ASCONSIT | Published on 05. May 2022

Secure passwords are an ongoing issue in IT. Whether private individuals or employees in companies or public institutions: Everyone needs passwords, every day. For example, when accessing an e-mail account, logging on to social media platforms or shopping online. But it's also a fact that not every password protects data equally well, and there will be no 100 percent security. All we users can do is try to make it as difficult as possible for an attacker. Unfortunately, in times of digitalization and the DSGVO, insecure passwords are still widespread. Yet secure passwords are very easy to generate and there are numerous aids for their creation and management. We have gathered the most important tips for you here.

Tip 1: Complex passwords

This tip should be familiar to everyone: use "strong" passwords whenever possible. But what exactly does strong mean? In the context of passwords, "strong" usually stands for passwords that are as complex as possible. Thus, when generating passwords, the way to go is: the longer, the more secure. Therefore, it is best to choose a password that consists of at least 14 characters and four-character types. At this length, even without numbers and special characters, the password can only be cracked in several years of brute forcing. By alternating upper- and lower-case letters and using numbers and special characters, password security can be increased even further.

Short password checklist

- At least 14 characters
- Alternation of upper and lower case letters (e. g. H, i, J, k)
- Numbers (1 ,2 ,3, ...)
- Special characters (space, ?, !, :, #)

In addition, avoid using consecutive characters e. g. "aaaa" or "1234abcd" as well as choosing a sequence of letters on the keyboard (e. g. xcvb, rtzu). Also, do not use obvious or familiar terms such as the names of family members, pets, friends, favorite stars, or birth dates. Single terms from the dictionary also offer insufficient protection. Only a combination of at least four words (more is even better) can create a secure password. You can select the individual words at random and combine them with a space or another special character to strengthen security.

Tip 2: An individual password for each access

Use different passwords for all accesses and accounts. While this does not make the password used more secure per se, it does minimize the damage if the password is hacked. If multiple accounts of a user are using the same e-mail address and one account is compromised, hackers will have an easy time with multiple passwords and access to all those accounts. Therefore, you should set an individual password for each account.

Tip 3: Password generator and manager

Our 3rd tip is to use a password manager. This tool stores passwords, which eliminates the need to remember every single password. That makes it much easier to use a different password for each account. Also, most password managers allow you to generate complex passwords. This ensures that the password cannot be cracked using a simple algorithm or the brute force method. It is best to install the password manager locally. By doing so, you do not give away the passwords because they are not stored in the cloud. For the master password, go for a strong password that protects access to the stored passwords. It is especially important to keep passwords a secret and not to tell anyone. For less relevant accounts (e. g. at Xing or LinkedIn), disposable passwords are suitable. This means that you use a password only once for each login and then renew it again (e. g., using the forgotten password function). It is best to check where data worth protecting is stored and can be viewed and where it is not. Passwords that protect sensitive data should only be entered on trustworthy computers anyway.

Tip 4: Change your password

Basically, it is important to know that changing the password regularly does not make the password itself more secure. Please refer to tip 1 once again. Nevertheless, it can be important to change the password. For example, if you suspect that your password has fallen into the hands of unauthorized third parties or your computer is identified with malware. You should then first clean up your device and then renew your credentials. After password recovery by a system or application, it is also a good idea to create a new password. After all, no one knows who may be able to read the automatically generated password.

Tip 5: Two-factor authentication

Nowadays, many platforms offer so-called two-factor authentication (2FA). By using 2FA authentication there is implemented another security level which makes it harder for possible intruders. Many people already know this from their e-banking account. The second factor is very variable (e. g., code via SMS, TAN generator), but it significantly increases access security.

How the brute force method works: The term brute force stands for the simple trying out of a large number of possible passwords by a hacker. Often, passwords are encrypted with cryptographic hash functions, because decrypting a password formed with an actual hash value method is practically impossible. However, the attacker can quickly calculate the hash values of many simple passwords. If a value matches the value of the stored password, he has decrypted the password. The brute force method always leads to success. It is only a question of time, because even a commercially available computer can test through several million combinations in one second. The best protection against a brute force attack is a long password with a high level of complexity, so that trying out all possible combinations becomes so time-consuming that the attack is not even worthwhile.

Conclusion: Users should attach importance to a password that is as complex as possible. If this is then for example changed on a quarterly basis, this significantly increases data security and protection against a cyber-attack. In addition, a password generator and manager help to create and manage passwords. All this ensures the protection of your identity in the internet and your data against attack in the best possible way!