HORNETSECURITY

INFOPAPER:
PASSWORD SECURITY CORRECTLY IMPLEMENTED

Content

Why password security is so important

Everyone knows the **basic recommendations on password security,** but very few people follow these guidelines. Instead, birth dates, names of children or keyboard shortcuts like „qwertz" or „123456789" appear regularly and are easily hacked.

Does this sound familiar? If so, your password habits should change quickly to make it as difficult as possible for hackers! A hacked password can quickly have serious consequences and lead to identity theft and financial losses. Hackers often succeed in **decrypting passwords with so-called brute force attacks.** Using certain tools, attackers simply try a large number of possible combinations. This method is guaranteed to lead to success, it is only a question of time. Even a standard computer can test several million such combinations in a second. How to successfully protect yourself against password theft is described below.

Safety first - Create secure passwords

Assuming an ordinary password consists of six characters and only lower case letters. This would be a maximum of 308,951,776 possible combinations that a brute force tool would have to try to decrypt the correct sequence of characters. That sounds like a lot - but it is possible in a few seconds. To really choose a secure password combination, the password should therefore consist of **12 to 16 digits.** Brute force attacks then have no chance. It is also important that the password contains **special characters such as commas or hyphens.** The Hornetsecurity experts strongly advise to also **use lower and upper case letters and numbers.** A secure password consisting of 16 characters would be, for example, „s~;u+.LT`"tmP?;y".

One password for all accounts - convenient but insecure!

The previously suggested password is **certainly not easy to remember** but such a complicated combination should be used. However, there is more to consider: Many users use the same password for many different accounts. If a cybercriminal gets their hands on that password, it would mean that they could access **email accounts, online banking accounts** or possibly even the **company network** with just one password. Therefore, only one individual password should be used per user account. This makes any attack much more difficult.

Forgotten your password? Choose security questions with care

Everybody has forgotten one or the other access code at some point. Fortunately, with most online services, the password can be reset by e-mail. One click is all it takes to set a new password via a confirmation link sent by e-mail.

There is also the possibility to **get access to your own account via the security question.** Questions like „What is the name of your pet?" or „How many children do you have?" are part of the standard repertoire. Many users appreciate this option very much. But in truth this is also a security gap. The selected security questions are **usually personal questions whose answers can be known to complete strangers** and can be hacked faster than the actual password. For this reason, it makes sense to select security questions whose answer is known only to yourself.

More and more often, online platforms are dispensing with this function. Google has not supported this type of recovery for a long time, and since 2019 the security question has not been asked for registration by the email providers GMX and Web.de, for example.

Password storage

The Hornetsecurity experts recommend that under no circumstances should the password be stored in a text file on the hard disk. Also, the automatic password storage in the browser should not be used. Because if the computer falls into the wrong hands, criminals have an easy game. Especially if you are in a public network, e.g. in a café or on the train, you must **make sure that third parties do not get access to your computer.**

HORNETSECURITY

The password manager as a solution

A big advantage for password security is a **password manager like KeePass.** It is a management software that allows passwords to be stored securely. Only a master key is needed to log into the program and access the other passwords. While this is practical, there are certain points to keep in mind:

The **master key** for the administration software should be a **password of 24 characters,** which is longer than average.

The master key should also use a **combination of letters, numbers and special characters** that has never been used elsewhere before.

Third parties and also persons who claim to be a trustworthy person or authority have no right to know the chosen password combination.

Checklist

If the above points are taken seriously, **cybercriminals will find it much more difficult to gain access to private accounts,** thanks to the high level of password security. Using the following checklist, everyone can regularly remind themselves of the most important aspects for secure password handling.

- ☑ The password should be **at least 12 characters** long, including special characters and upper and lower case letters.
- ☑ Use **one password for one account** only.
- ☑ Only select personal security questions whose **answers nobody can find out.**
- ☑ Do **not save passwords in text files** on your computer or in the browser.
- ☑ **Never share passwords** with other people.
- ☑ Use a **password manager** like KeePass.