27.01.2023

Are your password practices secure?

Users are not given an exactly clean bill of health by security researchers: In spite of all awareness campaigns, a large majority is still using weak passwords.

A current article published in the PCtipp computer magazine was headlined “The silliest passwords of 2022”. Similar to previous years, the “123456” character string still held the inglorious first place in the most popular passwords charts collated by the Hasso-Platner-Institut (HPI) each year. The other passwords making the top ten were little better. This latest analysis was based on over a million leaked access data.

Simple passwords are easy to remember – but even easier to crack. It takes any commonly available computer less than a minute to crack that “123456” password.

But just why are awareness campaigns advising on the correct use of passwords seemingly of so little avail? Studies like the “Psychologie der Passwörter” (Password psychology) by password manager suppliers LastPass try and provide an explanation. As per their research, the overwhelming majority of those questioned are convinced they are well-versed as far as passwords are concerned and 73% consider their passwords to be secure. Still: 69% say they are at least using strong passwords for their e-banking – dropping to a mere 38% as far as social media are concerned.

Generational differences also play a role. It is particularly younger users who use risky password practices without even realising. One thing which is striking: Across all the age groups, all those things learned during security training sessions is only put into practice inadequately or not at all.

This can be remedied by using passwords managers, for instance KeePass, as they simplify the administration of all those – frequently quite numerous – access data, no matter how complex and hence secure they are. Further information on how to use passwords securely can be found here (https://www.ebas.ch/step4#passwords) .