"Change Your Password Day" on February 1st

Also this year emphasizes the Bavarian State Commissioner for the

Privacy the importance of choosing secure passwords and gives

tips on this

Munich, January 31, 2019

February 1st is Change Your Password Day again.

For many years, "stolen" access data has been

published or sold for accounts. In many cases it will

facilitated by insufficiently secure passwords. That also shows

most recent publication of data, for example from politicians and journalists

listen. Nevertheless - as in the previous year - the sequence of numbers "123456"

the list of the most popular German passwords created by the Hasso

Plattner Institute is published each year.

Petri: "Just imagine what it means for you personally

would mean if your data was insecure, easily damaged

passwords fall into the wrong hands. As a result, can also

sensitive data may be affected, such as bank details

or private chat content. Well-chosen passwords are a building block

which you can contribute to the protection of your data. I encourage you-

Please use the "Change your password tag" to change your access data

to make it safer. Protecting your privacy is worth a little

time to invest."

What you should pay particular attention to when choosing passwords:

•

Use passwords with at least eight characters. To use

Please also use upper and lower case letters, digits and special

sign.

Your personal rights - our mission

The Bavarian State Commissioner for Data Protection informed

•

Avoid passwords that are directly related to you, such as

the name of family members or a pet.

•

•

•

•

•

Avoid passwords that consist of characters that are on the

keyboard next to each other (e.g. "123456" or

"QWERTZ").

Avoid (pass)words that are in the dictionary or in another

dictionary are listed.

Do not use the same password for different services.

Change default passwords.

Reduce the security of the password you choose

not with a simple answer to a security question that

Allows password reset. Do not use any in-

information that is easy to guess or otherwise research

are, such as names of family members.

Use the two-

factor authentication. This usually means that next to the

Password is another independent factor required to login.

This can be a further authentication via an SMS

transmitted PIN or possession of an object such as a security

trade health tokens.

If you have additional accounts for credential reset

use, protect them with strong passwords as well.

Delete accounts and all data on Internet services that you

no longer need.

Prof. Dr. Thomas Petri

The Bavarian State Commissioner for Data Protection checks the Bavarian public

public bodies compliance with data protection regulations. It's from Bavarian

Elected to the state parliament, independent and not bound by instructions from anyone.