HowTo Good Passwords

WPIA℠

WORLD PRIVACY AND IDENTITY ASSOCIATION

2020-06-08

Contents

1 What do I need to know?

This HowTo gives a simple overview about “secure passwords”.

Due to the complexitiy of passwords and their usage this HowTo is in no way complete and should be a help and guideline.

This matter is always to be taken in account and it is advisable to act with particular attention.

Passwords are used to secure IT devices and data. They avoid unauthorised access. Therefore the corret choice and handling is an urgent matter!

Especially IT security als well as the data protection are underlying continous changes. Therefore an advice from toyda can be obsolete tomorrow.

2 Passwords and tehchnical security

The choice of a good password is important for the security and privacy of data.

Good passwords have a sufficent length (at least 10 characters) and consists out of different types of characters like lower and upppercase letters, numbers and symbols which togehter should not combine to an usefull word.

Alternately suufcient long and individuell passphrases can be used.

In general the login password is the first and important protection of a computer tehaft or manipulation of any kind.

For the login to internet services as webmail, Facebook, ebay. PayPal and online banking never use the same password. If one of these thervise is compromised the attacker will have access to all internet services.

3 The correct usage

Passwords - especially the one to login to a computer - should never be exposed to someone else. Not even to colleages or supiriors. If handover of the password is needed, it must be changed immediately afterwards.

For different logins use different passwords. Small variations - e.g change three letters of the password - are still be remebered easily.

Nener use the same password for the computer and internet login.

4 The correct choice

Here only a short overview can be given.

- Minium length of 10 characters

- Random characters (taken from lower and upppercase letters, numbers and symbols). The use of only lower and upppercase letters is not secure!
- Never use names, first and last names, date of birth, number plates and similar person related data! They are chosen during an attack at first glance.
- Never take any entry from a dictonary (also not from a different language). As well proper name and geographical terms shoul not be used.
- The password is olny known by oneself.
- The password is used only for one application.
- Ideally the password can be remebered easily; alternately a password manager can be used which enable the use of complex passwords.
- Trivale passwords (e.g. qwerty, 12345678) are absolute unsuiteable. These can be easily be observed while entering through others.

5 How to generate a secure password?

5.1 Short Version:

Use a password generator!

5.2 Detailed Version:

Good password stay and fall with the randomness tehy are generated. Evedential humans are always underlying outer influences and cannot act randomly. These outer influences effect mostly unconsious for humans and therefore man made random passwords are not really random. They can be guessed quite easily.

5.2.1 Password length

There can be a proper discussion about the length of passwords.

The German Federal Office for Information Security (BSI) advises a general minimum length of 8 characters.

A minimum length of 12 - 14 charctarss are given by IT experts.

This advise are in contradiction to the usage in some internet services as many restrict the number of charcters. even current onlie banking portals only allow a login password with 5(!) charatcers.

There is an animous oprion that passwords witha lengt of 15 or more characters should be secure enough for everyday use. More charcters in a password give theoratical more combinations.

5.2.2 Characters of a password

A secure password should be as random as possible.

It is give that huamns are not good in creating randomnes.

A password should constists out of a large variety of different characters taken from lower and upppercase letters, numbers and symbols. The combination together with length are most important for the password security.

The password should never be taken from a -not eveb an foreign language - dictonary, should not conatin personal information loke names, profession, date of birth, number plates and telefon numbers. These data can be easily obtained and are used at first glance.

Also trivial passwords like letter series on the keyboard (qwerty) are a quite unsecure choice. They can be easily guessed.

5.2.3 Secret password

No one except oneself should know a password!

A password manager / password safe can be used so not each password needs to be remembered.

5.2.4 Unique password

For different application use different passwords. Never use the same password for different applications!

The most secure password is useless if it is used for different applications and one service is compromised. A hacker will use the obtained data to get access for further applications.

5.2.5 Easy to remember password

A password should be constructed in away that it can be remembered easily.

An alternative is the socalled acronym method. Here you take a long sentence, even with an individual and personal context. It should not realy make sense but should be easy to remember. Take the initials of each word and combine them to the password.

```
Example:
    I only can remember one password!
goes to password
    Iocr1pw!
```

5.2.6 Use password manager

With a password manager many different password can be managed in a secure way with one master password.

This password should be secure with the above criteria.

Many password manager offer to use a key file or security token instead of a master password,

The application stores the passwords encrypted on the computer. After entering the master password (to unlock the safe) all passwords are accessable. Some password manager generate passwords with one click.

There are many free application avaliable in the interent. USe open source software if possible.

If the web browser integrated password manager is used choose the matser password option.

The alternative would be - quite analog - paper and pen. The danger of unauthorised access is even larger.

Very important passwords should be remembered in your mind, but should also be store in a safe manner e.g. password safe.