NAWA Media

Securing Your Account

Section: 4.1

Strong Passwords, Strong Security

Passwords are the keys to your accounts and devices.

Strong passwords can mean the difference between hacking and safe enjoyment of your account.

Most people know what a strong password looks like but we'll go over the basics and some tips we believe to work in making awesomely secure passwords.

Basics of Strong Passwords

- It needs to be 18-12 characters long. Characters include alphabets, numbers, and special characters (#!@*&).
- Do not use words from the English language, and if you do replace some alphabets with special characters or numbers, like instead of a use @.
- If you can, make passwords in your own language, spelling them out in Roman English.
- Change your passwords at least once a month.

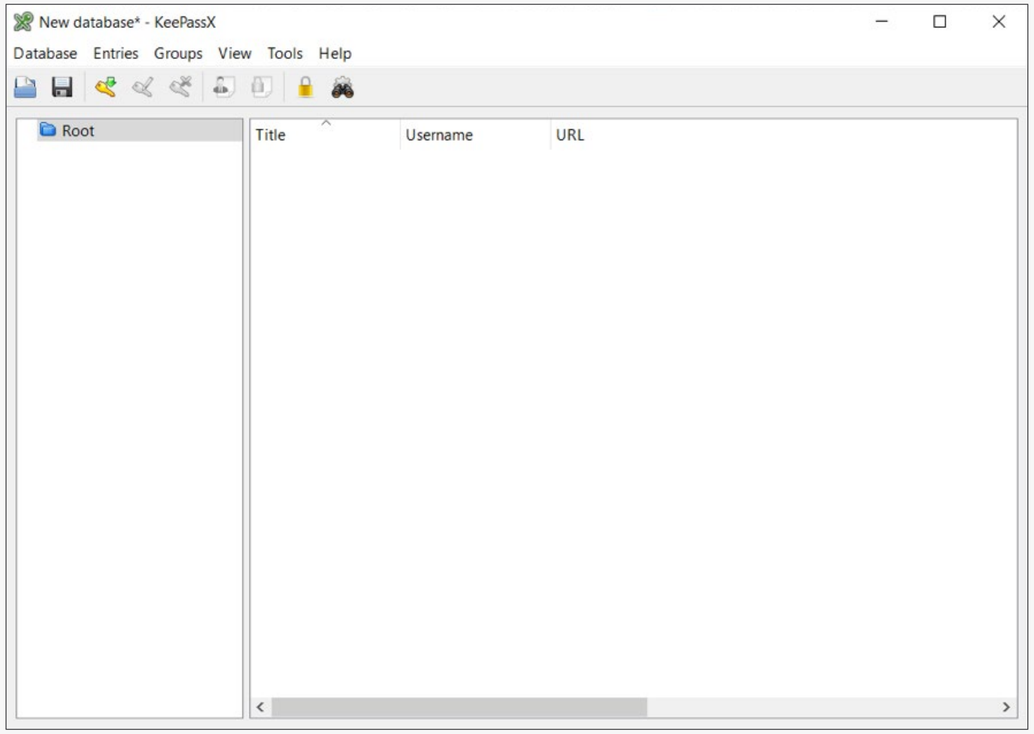
Your passphrase should not:

- be based on personal, easy-to-guess information such as birthdays, pet names etc.
- be based on personal likes and dislikes or hobbies
- be written down on a piece of paper or a document on your device

Password Storage: KeePass

If you need help generating and saving passwords, you can use a password manager like KeepassX. The only password you'll have to remember when using this is the password for your file.

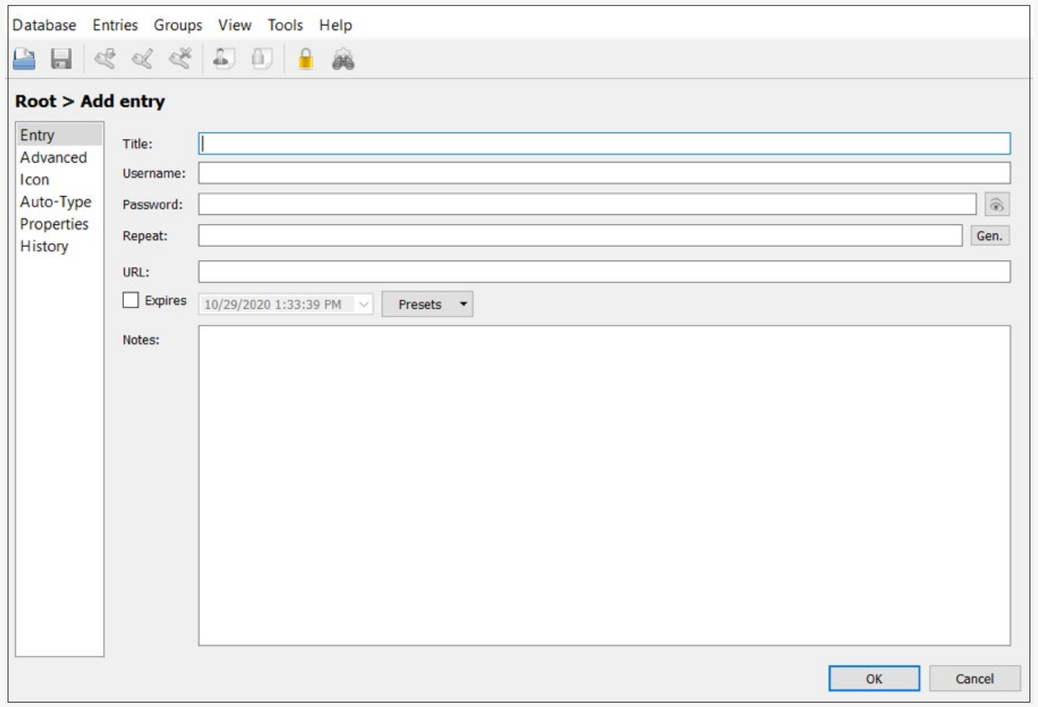
When you make a database on Keepass it looks like this:



Password Storage: KeePass

On the left hand side, you can right and create further subdivisions, and on the right side, you can right click and start entering passwords.

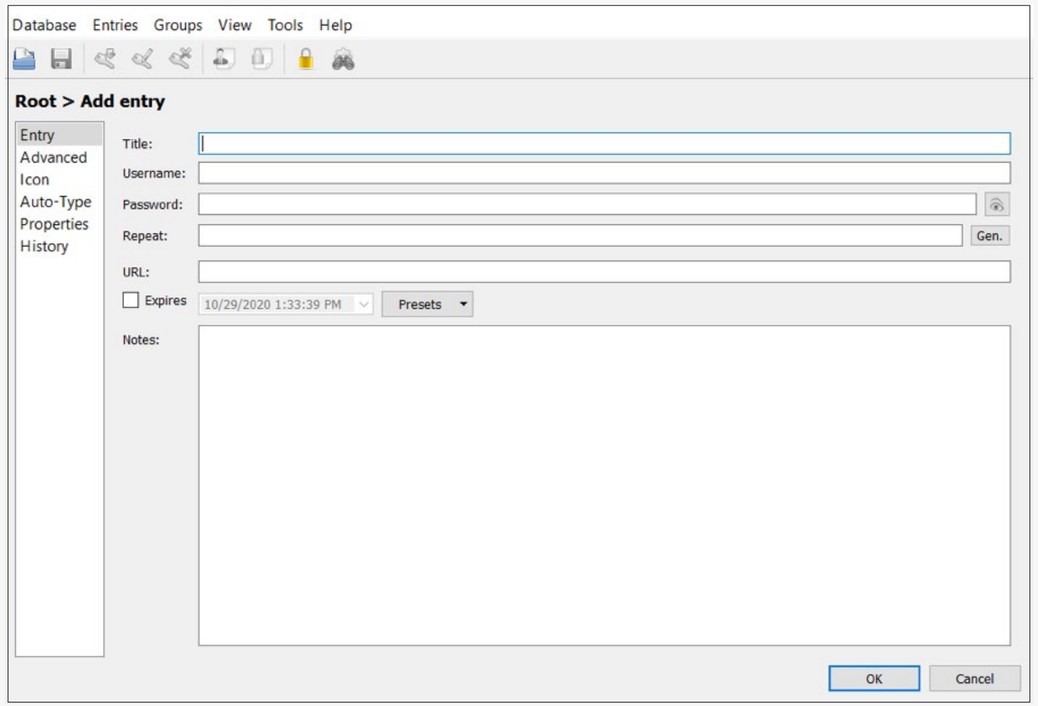
Once you start an entry it will look like the image on the right:



Password Storage: KeePass

In the middle right, you will spot a black dice icon. Clicking that will allow you to see the random password generator in the Keepass. You can control the length of the password and the types of characters you want to include in it. Once you press ‘OKAY’ the entry will be made.

When it comes to actually changing your password you will have to do that manually. Keepass is an offline tool which is what makes it safer than online password managers. Online managers are susceptible to the same threats all websites and apps online are. The only major risk the offline tool faces is the theft of the device the tool is installed on, or if the device fails entirely. This is where backups of your databases become relevant.



Two-Factor Authentication (2FA)

2FA is an added layer of security you can add on after your password. It is basically a prompt for you, the user, to enter a four to six digit code that, ideally, only you should have access through, either through your phone number (via SMS) or through an authenticator app. It allows you to be sure that only you have access to your account. It is also a great way for you as the user to know when someone has hacked your password and is trying to enter your account. They won't be able too since you've enabled 2FA.

All social media platforms and GMail have the option of enabling 2FA on your accounts. It is now almost a necessity to have 2FA on your accounts since password hacking has become more and more commonplace.

Using your mobile number as the recipient of your 2FA codes is generally okay however if you want to be super safe you can use authenticator apps like the Google Authenticator. These apps can be attached to your multiple accounts and every minute they will automatically generate new codes for your 2FA, making it even harder for people who want to gain access to crack the code.

NAWA Media

The **next** and last will introduce you to phishing attacks and how to prevent them.

BCMCR | Birmingham Centre for Media and Cultural Research

BIRMINGHAM CITY University

MEEDAN

Check

Sida