Is Roboform Password Saver Safe?

Author:
Resale Rights

Created On: 11 Feb 2010 03:35 AM

It is very safe and secure.
Your Identities and Passcards are encrypted using AES, BlowFish, RC6 or 3DES algorithm and the encryption / decryption key is generated from the Master Password. This encryption method makes your data very secure and even if hackers come into possession of your Identity and Passcard files, they will have to crack one of these encryption algorithm without knowing the key which is considered impossible. By default AES encryption is used.

What is the 3DES encryption standard?

Triple Data Encryption Standard (3DES) is the most common encryption standard used in the enterprise today. 3DES is where 3 different 56 bit keys are used to encrypt the data three times. 3DES uses a 168 bit key, which is long enough that it is not easy to break. It is most commonly used in Virtual Private Networks.

What is the AES encryption standard?

AES stands for the Advanced Encryption Standard. It uses 128 bit symmetrical blocks to encrypt the data. So you can have AES128, AES256, AES384, etc. by increasing the key size by 128 bits. It has been adopted by the United States Government as its official standard for encrypting data.

What is the Blowfish encryption standard?

Blowfish is an open source encryption standard that is used in Linux applications such as Secure Shell (SSH). It supports encryption keys of varying lengths, with 512 and 1024 the commonly used lengths. It is optimized to run on 32 bit operating systems, so it encrypts and decrypts faster than many other encryption standards. Since it is an open source (freely available) solution, many developers have adopted it.Â

Â

Click Here to Download a **Free Trial of RoboForm**